RSA og den heri anvendte matematiks historie

et undervisningsforløb til gymnasiet

Jankvist, Uffe Thomas

Publication date:
2008

Document Version
Også kaldet Forlagets PDF

Citation for published version (APA):
Jankvist, U. T. (2008). *RSA og den heri anvendte matematiks historie: et undervisningsforløb til gymnasiet*. Roskilde Universitet. IMFUFA-tekst : i, om og med matematik og fysik Nr. 460

IMFUFA tekst

- I, OM OG MED MATEMATIK OG FYSIK

RSA og den heri anvendte matematiks historie - et undervisningsforløb til gymnasiet

Uffe Thomas Jankvist
januar 2008

nr. 460 - 2008

blank

Roskilde University,
Department of Science, Systems and Models, IMFUFA
P.O. Box 260, DK - 4000 Roskilde
Tel: 4674 2263 Fax: 4674 3020

RSA og den heri anvendte matematiks historie
– et undervisningsforløb til gymnasiet
Af: Uffe Thomas Jankvist, januar 2008

IMFUFA tekst nr. 460/ 2008 – 116 sider – ISSN: 0106-6242

For faget matematiks vedkommende stiller den gymnasiale bekendtgørelse af 2007 krav om at der som del af undervisningens supplerede stof behandles elementer af matematikkens historie, eksempelvis gennem matematikhistoriske forløb. Nærværende tekst indeholder undervisningsmateriale designet til et sådant matematikhistorisk forløb.

Et af formålene med materialet har været overfor eleverne at belyse nogle af de sider af matematikkens udvikling som KOM-rapporten (Niss & Jensen, 2002) nævner. Eksempelvis at matematikkens udvikling finder sted i tid og rum, at den udvikles af mennesker og ikke blot opstår ud af ingenting samt at udviklingen drives af såvel interne som eksterne faktorer.

I første kapitel af teksten gives en introduktion til såvel privat- som offentlig-nøgle kryptering, også kaldet symmetrisk og asymmetrisk kryptering, samt det såkaldte nøgledistributionsproblem. Herefter præsenteres i kapitel 2 og 3 det talteori som er nødvendigt for at forstå den specielle form for offentlig-nøgle kryptering der kendes som RSA. Korrektheden af RSA-algoritmen hviler på tre matematiske sætninger fra talteorien, den kinesiske restsætning, Fermats lille sætning og Eulers sætning, hvor Eulers sætning er en generalisering af Fermats. Formålet med kapitlerne 2 og 3 er således at udvikle den nødvendige matematik, herunder diverse talteoretiske begreber, for forståelsen af disse sætninger samt deres beviser. Præsentationen af selve RSA-algoritmen finder sted i kapitel 4.

Samtidig med at de matematiske forudsætninger for RSA opbygges og præsenteres fra bunden fortælles også historien bag disses tilblivelse, eksempelvis de relevante dele af Gauss', Fermats og Eulers talteoretiske arbejder. Mest bliver der dog gjort ud af den nyere krypterings historie. Det vil sige Diffies og Hellmans ide til den offentlige-nøgle kryptering, Rivest, Shamirs og Adlemans realisering af denne samt den parallelle udvikling i den britiske efterretningstjeneste – begivenheder som stort set alle fandt sted i løbet af 1970'erne. Der er altså i høj grad tale om en *moderne anvendelse* af noget flere hundrede år gammelt matematik, og i KOM-rapportens termer tilmed en anvendelse hvis udvikling i høj grad blev drevet af eksterne faktorer.

For at sikre at eleverne selv går i dybden med de historiske aspekter af den præsenterede matematiske kryptering afsluttes forløbet med en såkaldt essay-opgave. Ideen er her, at eleverne i grupper arbejder med at besvare en række stillede opgaver, at de anvender de (matematikhistoriske) værktøjer som stilles til rådighed herfor og at det hele munder ud i en skriftlig rapport (lidt i tråd med en dansk stil). Materialet indeholder også et antal såkaldte historiske opgaver, hvor eleverne præsenteres for og forventes at arbejde med oversatte uddrag af matematikhistoriske originalkilder.

Forløbet om RSA og den heri anvendte matematiks historie er som led i min ph.d. blevet implementeret i en 3g-klasse på Ørestad gymnasium i efteråret 2007. Klassens egen matematikunderviser gennemførte forløbet, mens jeg observerede og videofilmede hele processen. Specielt fulgte jeg én gruppe bestående af fem elever i forbindelse med deres arbejde med den afsluttende essay-opgave. Resultaterne af denne undersøgelse vil blive fremlagt i min ph.d.-afhandling som forventes afsluttet i midten af 2009.

Uffe Thomas Jankvist, 2008

Forord

Ligesom undervisningsmaterialet om kodningsteoriens tidlige historie og forløbet i forbindelse dermed er dette undervisningsmateriale og -forløb også en del af min ph.d. i matematikkens didaktik og historie ved Roskilde Universitet. Ph.d.-projektet omhandler brugen af matematikkens historie i matematikundervisningen, hvilket er særlig aktuelt i forbindelse med den ny bekendtgørelse for gymnasiet. For matematik hedder det heri under punktet »formål«:

> Gennem undervisningen skal eleverne opnå kendskab til vigtige sider af matematikkens vekselvirkning med kultur, videnskab og teknologi. Endvidere skal de opnå indsigt i, hvorledes matematik kan bidrage til at forstå, formulere og behandle problemer inden for forskellige fagområder, såvel som indsigt i matematisk ræsonnement. (Undervisningsministeriet; 2007)

Ydermere opstilles der en række »faglige mål« som eleverne vil blive 'målt og vejet' i forhold til. Disse skal dog ikke udelukkende opnås ved hjælp af »kernestoffet«, men også gennem såkaldt »supplerende stof«. Det hedder:

> For at eleverne kan leve op til de faglige mål, skal det supplerende stof, der udfylder ca. 1/3 af undervisningen, bl.a. omfatte [...] matematik-historiske forløb. (Undervisningsministeriet; 2007)

Det »faglige mål« som matematikhistoriske forløb retter sig mod lyder:

> Eleverne skal kunne [...] demonstrere viden om matematikkens udvikling i samspil med den historiske, videnskabelige og kulturelle udvikling. (Undervisningsministeriet; 2007)

Det matematikhistorie som I, eleverne, vil blive udsat for i dette forløb er at betegne som en *moderne anvendelse* af historisk matematik, hvilket i denne sammenhæng vil sige at meget af matematikken er ældgammel, men selve anvendelsen af den først kom i stand i 1970'erne. Mere præcist er der tale om matematisk *kryptering* af information, hvilket vil sige en indkodning af en given meddelelse med det formål at hemmeligholde denne. Helt præcist er der tale om den type kryptering der kendes under betegnelsen *RSA-kryptering*. Denne type kryptering udnytter visse egenskaber ved de naturlige tal og specielt de af disse der kendes som primtal. Studiet af primtal, deres forskellige egenskaber og deres relationer til de hele tal iøvrigt kan spores langt tilbage i historien, eksempelvis til Euklids *Elementer* fra omkring år 300 f.v.t.

I den af Undervisningsministeriet sponserede KOM-rapport (Kompetencer Og Matematiklæring), som den ny bekendtgørelse for matematik i gymnasiet i nogen grad bygger på, gives der følgende forslag til eksemplificering af matematikkens historiske udvikling:

> Primtallene – hvordan ren matematik pludselig bliver til anvendt matematik, og hvorfor det er fornuftigt at investere i grundforskning. (Niss & Højgaard Jensen; 2002, side 268)

Det her givne undervisningsmateriale om RSA-kryptering og den heri anvendte matematiks historie kan ses som en realisering af KOM-rapportens eksemplificering ovenfor.

En essentiel del af dette undervisningsmateriale er den *afsluttende essay-opgave*, som består af et antal skriftlige (essay-)opgaver, samt de såkaldte *historiske opgaver* som figurerer løbende igennem materialet. Der skal i forbindelse hermed gøres opmærksom på, at en besvarelse af essay-opgave 74 forudsætter at man har læst G. H. Hardys *A Mathematician's Apology* (eller for opgaven relevante uddrag heraf). Læsningen af denne tekst kan eventuelt foregå i engelskundervisningen som en del af det samlede undervisningsforløb, dermed realiserende nogle af de tværfaglige aspekter den ny bekendtgørelse også lægger op til.

Teksten i undervisningsmaterialet er sat med to forskellige fonte; denne til matematik, og den her anvendte til kommentarer, såvel historiske som anvendelsesorienterede. Dette tiltag er tænkt som en service for læserne. Da det behandlede stof i undervisningsmaterialet er mere bevistungt end elever i stx muligvis er vant til er der indført endnu en service: De af beviserne som måske godt kan tåle at blive sprunget over er markeret med en stjerne (Bevis*). Selvfølgelig er det op til den enkelte underviser, at bestemme sig for hvilke beviser som er de vigtige og de mindre vigtige, men materialet byder altså på en form for 'guideline' i denne henseende. Og det samtidig med at alle beviser er præsenteret til ære for den interesserede læser.

Oktober, 2007
Uffe Thomas Jankvist
IMFUFA, Roskilde Universitet

Indhold

1 Introduktion

Igennem tusinder af år har menneskene haft et behov for at kunne kommunikere med hinanden uden at indholdet af deres sendte meddelelser kunne blive læst af udenforstående parter. For eksempel i forbindelse med krig, i forbindelse med kærlighedsaffærer, eller i forretningsøjemed er det ofte relevant at kunne afsende og modtage hemmelig information. Historien byder således på et hav af eksempler til måder at løse dette problem på og med tiden har det at kunne indkode og afkode hemmelig information udviklet sig til en hel videnskab. Denne videnskab kaldes *kryptering* efter det græske ord kryptos som betyder hemmelig. Videnskaben om kryptering kaldes også gerne for enten *kryptografi* eller *kryptologi*, og de der beskæftiger sig med denne videnskab kaldes derfor for *kryptografer* eller *kryptologer*. Kryptografers (eller kryptologers) arbejde består i at opstille såkaldte *kryptosystemer*, det vil sige systemer inden for hvilke kommunikation af hemmelig information kan foregå på sikker vis. Et kryptosystem består i bund og grund af to procedurer, en kaldet *kryptering* og en kaldet *dekryptering*. Kryptering, undertiden også refereret til som *(ind)kryptering*, består i at kode den hemmelige information før denne afsendes til en given modtager. Dekryptering består i for modtageren at afkode den hemmelige information tilbage til den oprindelige meddelelse. Et af de tidligere historiske eksempler på et kryptosystem er det der blev anvendt af den romerske kejser Gaius Julius Cæsar (100 f.v.t.-44 f.v.t.) og som derfor i dag er kendt som *Cæsar-kryptering*. Dette systems metode til (ind)kryptering består i at udskifte bogstaverne i en meddelelse med de bogstaver som står tre pladser længere fremme i alfabetet. Et eksempel på Cæsar-kryptering kunne være følgende:

TERNINGERNE ER KASTET → WHUQLQJHUQH HU NDVWHW.

Den krypterede tekst, den på højresiden af pilen, kaldes gerne for *krypteksten*. Hvis der i en meddelelse indgår bogstaver fra de tre sidste pladser i alfabetet vil disse blive udskiftet med dem i begyndelsen af alfabetet. Altså, Æ, Ø og Å vil blive til henholdsvis A, B og C. Dekryptering består for modtageren i at udføre den omvendte procedure, altså at udskifte bogstaverne i den modtagne meddelelse med dem der står tre pladser tidligere i alfabetet. Dekrypteringen bliver således:

WHUQLQJHUQH HU NDVWHW → TERNINGERNE ER KASTET.

Ligesom kryptering udgør en videnskab så udgør også det at bryde eksisterende kryptosystemer nærmest en hel videnskab. Denne videnskab kaldes for *krypto-*

analyse og de folk der beskæftiger sig dermed kaldes for *kryptoanlytikere*, eller med et mere jævnt navn blot *kodebrydere*.

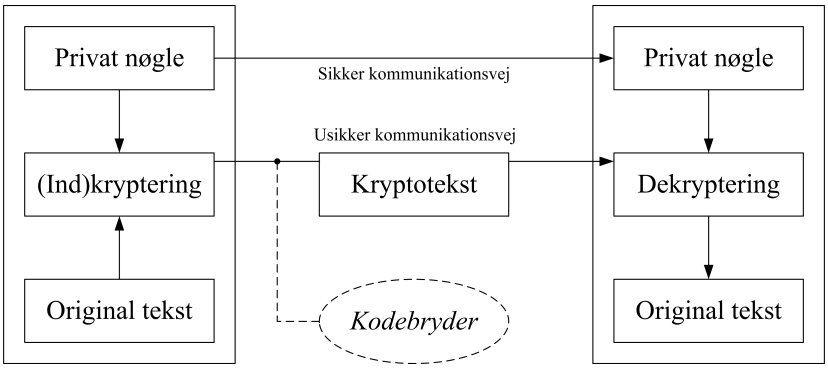
Vi skal i dette kapitel se nogle eksempler fra kryptografiens historie på henholdsvis kryptering og kryptoanalyse. Disse eksempler tjener som en introduktion til området og ikke mindst som en måde at få en forståelse for nogle af de problemer som kryptografer og kodebrydere har måttet kæmpe med for henholdsvis at opretholde sikre kommunikationsveje, i form af sikre kryptosystemer, eller for at knække disse systemer og derigennem få indsigt i de hemmelige meddelelser som blev transmitteret ad disse veje. Introduktionen og den historiske gennemgang er struktureret i forhold til de to typer af kryptosystemer som man inden for kryptografien normalt skelner imellem; *privat-nøgle kryptering* og *offentlig-nøgle kryptering*. Ofte omtaler man de to procedurer til henholdsvis (ind)kryptering og dekryptering som et kryptosystem består af som *algoritmer*. Med begrebet algoritme menes der inden for matematik (og datalogi) noget helt bestemt og en diskussion af hvad vi vil, og ikke vil, forstå ved en algoritme er derfor også på sin plads og findes i det sidste afsnit af kapitlet.

1.1 Privat-nøgle kryptering

Cæsar-kryptering, som vi fik beskrevet ovenfor, er et eksempel på en såkaldt *privat-nøgle kryptering*. Denne betegnelse kommer af, at man for at være i stand til såvel at (ind)kryptere som at dekryptere en besked må være i besiddelse af en nøgle. I tilfældet med Cæsar-kryptering er nøglen til (ind)kryptering at flytte bogstaverne tre pladser frem i alfabetet og nøglen til dekryptering er, at man skal flytte bogstaverne tre pladser tilbage. Disse nøgler er *private* fordi de skal hemmeligholdes overfor dem som kunne være interesserede i de (hemmelige) meddelelser man sender. Hvis nøglerne enten opsnappes eller på anden vis bliver offentligt kendt vil kryptosystemet ikke længere være at regne for sikkert. Privat-nøgle kryptering kendes også ofte under navnet *symmetrisk kryptering*. Dette navn skyldes, at de processer der må udføres af afsenderen afspejles af dem der må udføres af modtageren. Dette er illustreret på figur 1.1. Med symmetrisk, eller privat-nøgle, kryptering forholder det sig ofte også sådan, at hvis man kender enten krypterings- eller dekrypteringsnøglen, så kender man også den anden af disse. Dette skyldes, at de to nøgler gerne er hinandens omvendte. I tilfældet med Cæsar-kryptering er krypteringsnøglen jo 'bogstav + 3 pladser' og dekrypteringsnøglen bliver så 'bogstav − 3 pladser'. I matematikken tænker man ofte på en kryptering som en matematisk funktion, lad os kalde den f, hvorved dekrypteringsnøglen bliver denne funktions *omvendte*. Den omvendte for funktionen $f(x)$ er defineret til at være den funktion, hvor der for ethvert y i f's værdimængde er præcist ét x i f's definitionsmængde som skaber dette y. Den omvendte funktion betegnes ved $f^{-1}(y)$. Pas dog på ikke at blande den omvendte funktion $f^{-1}(y)$ sammen med brøkfunktionen $1/f(y) = (f(y))^{-1}$, selv om skrivemåderne minder om hinanden har disse to funktioner intet med hinanden at gøre. Situationen her stiller så selvfølgelig det krav til

krypteringsprocessen, at denne skal kunne beskrives ved en matematisk funktion og tilmed en funktion som har en omvendt (hvilket ikke gælder for alle funktioner).

Som man nok kan tænke sig til er Cæsar-kryptering en meget simpel metode til kryptering og et kryptosystem baseret på Cæsar-kryptering kan da også forholdsvist let brydes. En helt oplagt metode til at bryde kryptosystemer baseret på substitutioner af bogstaver, sådan som Cæsar-kryptering er, består i at foretage en *frekvensanalyse* af de indgående tegn – en metode udviklet af arabiske kryptografer i det 9. århundrede. I eksemplet ovenfor kan vi tælle frekvensen af de indgående tegn, altså antallet af gange de enkelte bogstaver optræder, i kryptoteksten: `WHUQLQJHUQH HU NDVWHW`. En sådan frekvensoptælling kan derefter bruges til at komme med kvalificerede gæt på hvilke bogstaver der er substitueret med hvilke andre. Eksempelvis bemærker vi at `H` optræder hele fem gange i kryptoteksten ovenfor. Bogstavet `E` er det oftest forekommende bogstav i det danske sprog, altså vil et kvalificeret gæt være at `H` er substitueret for `E`. Sådan kan man så fortsætte med at analysere og gætte sig frem og jo flere bogstaver i kryptoteksten man får afkodet jo nemmere bliver det at gætte den samlede meddelelse. I tilfældet med Cæsar-kryptering er det så ydermere nemt, idet substitutionerne er foretaget efter den samme faste regel. Har man således først fået øje på et mønster i den krypterede besked og afkodet krypteringsfunktionen f står kryptosystemet for fald. Kryptosystemer som kan brydes ved hjælp af frekvensanalyser, sådan som Cæsar-kryptering kan, anses for at være blandt de allermest usikre kryptosystemer overhovedet. Men som historien viser gik der en rum tid førend dette gik op for samtlige kryptografer, hvilket vi skal se lidt nærmere



Figur 1.1 Symmetrisk eller privat-nøgle kryptering: Den originale tekst (ind)krypteres ved hjælp af den private nøgle givende kryptoteksten. For at den private nøgle forbliver privat overdrager afsenderen af beskeden nøglen via en sikker kommunikationsvej til modtageren. Kryptoteksten sendes imidlertid via en usikker kommunikationsvej, hvilket giver eventuelle kodebrydere mulighed for at opsnappe denne. Modtageren dekrypterer kryptoteksten ved hjælp af den private nøgle og får derved den originale tekst.

på nu.

I løbet af 1500-tallet begyndte de europæiske hoffer at ansætte talentfulde kryptoanalytikere.[1] Specielt det franske hof havde nogle usædvanligt dygtige kodebrydere ansat, heriblandt den franske matematiker François Viètes (1540-1603). Viète nød stor respekt for sine talenter som kryptoanalytiker og ikke mindst for sine brydninger af spaniernes krypterede meddelelser. At de spanske krypteringer forekom Viète så ligetil at knække kom vældigt bag på Spaniens kryptografer, og ikke mindst den spanske konge Philip II. Kongen gik tilmed så vidt som til at melde Viète til Vatikanet. Anklagen lød på at Viète måtte stå i ledtog med djævlen, for hvordan skulle han ellers være i stand til at bryde Spaniens 'ubrydelige' koder. Philip II krævede derfor Viéte stillet for retten for sine 'dæmoniske handlinger'. Paven var imidlertid bedre informeret, idet hans egne kryptoanalytikere også forstod at tyde de spanske beskeder, og han afslog derfor Philip II's anklage. Sagens kerne var den, at de spanske kryptografer baserede deres krypteringer på såkaldte *monoalfabetiske* substitutioner, hvilket vil sige at man kan opskrive krypteringsnøglen som to rækker; den øverste bestående af det almindelige alfabet og den nedenunder af substitutionsalfabetet. I Cæsar-krypterings tilfælde vil der under `A` således stå `D`, under `B` stå `E`, under `C` stå `F`, og så videre. De fleste andre steder i Europa havde man på dette tidspunkt fået øjnene op for sådanne krypteringers svage punkt, nemlig frekvensanalyse. Man var derfor gået over til såkaldte *polyalfabetiske* substitutioner i stedet. Her opskrev man under rækken med det almindelige alfabet adskillige substitutionsalfabeter. I (ind)krypteringen varierede man så imellem disse, i overenstemmelse med et eller andet aftalt mønster som udgjorde nøglen. Dette gjorde det væsentlig sværere for kryptoanalytikere at bryde de krypterede beskeder. Det mest udviklede af sådanne kryptosystemer var *Vigenère-koden*, opkaldt efter dens opfinder Blaise de Vigenère (1523-1596). Systemet bestod af lige så mange substitutionsalfabeter som der var bogstaver i alfabetet; første substitutionsalfabet var lig det almindelige alfabet, andet substitutionsalfabet var lig det almindelige flyttet en plads mod højre, det tredje var lig det almindelige flyttet to pladser mod højre, og så videre (se opgave 10). Vigenère-koden forekom at være immun overfor frekvensanalyse (hvorfor?), og den blev derfor kendt som *Le Chiffre Indéchiffrable*. Ikke førend i midten af 1800-tallet blev koden knækket. Det var den engelske videnskabsmand og matematiker Charles Babbage (1791-1871), opfinderen af flere af de grundlæggende principper i vore dages computere, der gav Vigenère-koden dødsstødet. Babbages metode var en udvidet form for frekvensanalyse, hvor han i den krypterede besked forsøgte at identificere mønstre forårsaget af forskellige indkrypteringer af gentagede ord i beskeden. Begivenheden fandt sted i 1854, men Babbage publicerede intet om sin metode til brydning af koden, hvilket muligvis skyldtes at den engelske efterretningstjeneste fik nys om denne og pålagde ham ikke at offentliggøre noget derom. Imidlertid blev samme metode fundet, uafhængigt af Babbage, i 1863 af en preussisk officer ved navn Kasiski, og metoden er i dag bedst kendt som Kasiski-metoden.

[1] Store dele af den historiske gennemgang i dette kapitel er baseret på (Singh; 1999).

Det næste halve århundrede havde kryptoanalytikerne, qua brydningen af Vigenère-koden, overtaget over kryptograferne. I 1918 begyndte situationen dog at ændre sig til kryptografernes fordel, idet den tyske opfinder Arthur Scherbius her opfandt den første udgave af den mekanisk-elektriske *Enigma*-kryptomaskine. Den oprindelige Enigma bestod af tre forskellige mekanismer: (1) Et tastatur med 26 bogstaver, hvorpå man trykkede på det bogstav som skulle krypteres. (2) Tre såkaldte rotorer som stod for krypteringen ved at lade det på tastaturet valgte bogstav blive udsat for tre på hinanden følgende substitutioner. (3) Og til sidst lystavlen, hvorpå det krypterede bogstav kunne aflæses. En rotor var en smal cylinder med 26 forskellige indstillinger, en for hver bogstav. Rotoren fungerede som substitutionsalfabet, blot med den markante forskel at den kunne rotere, hvilket i realiteten betød at den fungerede som 26 forskellige substitutionsalfabeter. Og da der var tre rotorer, som alle kunne rotere, blev der således tale om at et bogstav kunne (ind)krypteres på $26 \cdot 26 \cdot 26 = 17576$ forskellige måder. Senere udgaver af Enigmaen havde også ombyttelige rotorer, hvilket bidrog med en faktor $3! = 6$ til regnestykket ovenfor. Tilmed blev der tilføjet en elektrisk tavle imellem tastaturet og rotorerne som gjorde det muligt at ombytte flere par af bogstaver inden disse blev krypteret – et tiltag som forøgede antallet af forskellige substitutioner med adskillige milliarder. Den Enigma som tyskerne anvendte under optakten til anden verdenskrig kunne således substituere et bogstav på $\approx 10^{16}$ forskellige måder. Startpositionen for rotorerne såvel som rækkefølgen af disse udgjorde sammen med ombytningen af bogstaver i den elektriske tavle krypteringsnøglen. Under krigen anvendte tyskerne en ny nøgle hver dag og hver måned distribuerede de kodebøger med dagsnøgler til samtlige Enigma-operatører.

De allieredes kryptoanalytikere stod i begyndelsen magtesløse overfor dette nye kryptosystem. Frekvensanalyse var blevet gjort endnu mere umuligt at anvende på grund af det enorme antal af substitutionsmuligheder. Men i takt med at den tyske værnemagt begyndte at udgøre en markant trussel blev flere og flere resourcer sat ind på at bryde Enigma-koden. Franskmændene havde allerede i 1931, ved at betale en tysk forræder, fået kendskab til designet bag Enigmaen. Imidlertid syntes de ikke interesserede i at forsøge at bruge disse informationer selv til at bygge en kopi af apparatet. Heldigvis videregav franskmændene deres viden om Enigmaen til polakkerne, som i kraft af den unge polske matematiker Marian Rejewski (1905-1980) var i stand til at identificere svagheder i såvel Scherbius' design som i tyskernes brug af maskinen. Fra først i 1930'erne og frem til 1938 var polakkerne således i stand til at læse samtlige af de tyske meddelelser de opsnappede, og det var mange, eftersom disse nu blev transmitteret med radio. I slutningen af 1938 øgede tyskerne imidlertid deres sikkerhedsniveau ved at tilføje to ekstra rotorer samt sætte antallet af ombytninger i den elektriske tavle op, resulterende i at antallet af substitutionsmuligheder nu steg til $\approx 159 \cdot 10^{18}$. Rejewski og de andre polske kryptoanalytikere måtte til sidst give fortabt. Da man dog på dette tidspunkt var sikker på at tyskernes angreb på Polen var nært forestående blev det besluttet, at franskmændene og englænderne skulle indvies i polakkernes brydning af Enigma-koden, noget som indtil

nu havde været hemmeligholdt. Frankrig og England modtog således hver en nøjagtig kopi af den tyske Enigma, som polakkerne havde bygget udfra franskmændenes videregivne informationer, samt tegninger for designet af den såkaldte *Bombe* – en maskine som Rejewski havde designet, fået bygget og brugt i brydningen af de tyske koder. Dette skete kun få måneder før tyskerne i 1939 besatte Polen.

Englænderne havde kort forinden oprettet et nyt center i Bletchley Park, som skulle arbejde på at bryde de opsnappede tyske meddelelser. Den fra vores synspunkt mest markante figur ved Bletchley Park var den unge engelske matematiker Alan Turing (1912-1954), hvis interesseområde lå inden for matematisk logik, men også omfattede flere områder af vore dages datalogi. Turing var i stand til at identificere nye 'huller' i tyskernes brug af Enigmaen, for eksempel daglige beskeder indeholdende ens formuleringer. Ligesom Rejweski fulgte Turing en strategi med at adskille rotor-krypteringen fra krypteringen forårsaget af den elektriske tavle. Dette forenklede processen væsentligt, idet han nu i første omgang kunne nøjes med at se på de $5! \cdot 26^5 = 1425765120$ forskellige rotorindstillinger, hvilket dog stadig var noget mere end de 105456 som Rejewski havde skulle behandle. Imidlertid formåede Turing at videreudvikle Rejewskis Bombe til at håndtere det højere antal af substitionsmuligheder. Men tyskerne blev ved med at ændre deres (ind)krypteringsstrategier igennem hele krigen, så folkene ved Bletchley Park havde nok at gøre med at tilpasse deres metoder til brydning af koderne.

Med fremkomsten af programmerbare computere, englænderne byggede Colossus i 1943 og amerikanerne ENIAC i 1945, fik kryptoanalytikerne igen overtaget over kryptograferne, da en computer nemt kunne gennemprøve samtlige muligheder af Enigma-nøgler. Enigma-koden såvel som andre lignende (mekanisk-elektriske) kryptosystemer var derfor ikke længere at regne for sikre. Men også kryptograferne fandt snart ud af at de kunne drage nytte af computeren og ikke mindst det faktum, at denne baserede sig på beregninger med binære tal (tal bestående af 0'er og 1-taller). Et af de mere berømte, og i nogen grad stadig anvendte, kryptosystemer baserende sig på binære beregninger er *Lucifer*. Denne kode blev udviklet af tysk-amerikaneren Horst Feistel (1915-1990) mens han i begyndelsen af 1970'erne var ansat ved IBMs Thomas J. Watson Laboratory. Uden at gå alt for meget i detaljer går Lucifer-koden ud på, at man først oversætter sin besked til binære tal, for eksempel ved hjælp af ASCII-alfabetet, og at man derefter deler strengen af 0'er og 1-taller op i mindre blokke. Tallene i disse blokke udsættes så for en såkaldt 'scrambler'-funktion som blander disse godt og grundigt sammen, hvorefter de resulterende blokke lægges sammen ved binær addition. Denne procedure gentager sig selv et vist antal gange, hvorefter beskeden er krypteret og kan sendes til modtageren. Krypteringsnøglen er et tal, som når det indsættes i scrambler-funktionen definerer den specifikke procedure som talblokkene skal udsættes for. I 1973 blev Feistels Lucifer-kode ophøjet til USAs Data Encryption Standard kode, hvorfor den i dag oftest omtales som *DES*.

En pointe som man kan fremdrage af de ovenfor præsenterede elementer af krytografiens historie går på den fremtrædende rolle som matematikere synes at spille inden for kryptoanalyse: Viète dechifrerede de spanske beskeder,

Babbage knækkede det 300 år gamle *Le Chiffre Indéchiffrable* (Vigenère-koden) og Rejewski og Turing fik bugt med tyskernes frygtindgydende Enigma-kode. Det synes altså at være matematikerne der bryder de 'ubrydelige' koder. Men er det også matematikerne som laver de 'ubrydelige' koder? Nej, historisk set lader det ikke til at have forholdt sig sådan. I løbet af 1970'erne begyndte der imidlertid at tegne sig et nyt billede, matematikerne syntes at skifte lejr, fra kryptoanalytikernes til kryptografernes. Og i den del af kryptografiens historie som vi skal beskæftige os med i dette undervisningsmateriale er det netop matematikere, herunder en speciel form for matematiske dataloger, som er ophavsmænd til de (indtil videre) ubrydelige koder.

1.2 Nøgle-distribueringsproblemet

Samtlige af de systemer vi har diskuteret ovenfor er alle underlagt et og samme problem: Problemet med distribution af de private nøgler, eller *nøgle-distribueringsproblemet* som det også kaldes. For eksempel skulle man i de monoalfabetiske kryptosystemer kende den funktion som definerede substitutionerne. I de polyalfabetiske kryptosystemer måtte man vide hvordan man varierede imellem de forskellige substitutionsalfabeter. For at anvende Enigma-koden måtte man kende den pågældende dagsnøgle angivende startpositionen for rotorerne, deres indbrydes rækkefølge samt ombytningerne i den elektriske tavle. Og i DES skulle man kende det naturlige tal som definerede den anvendte scrambler-funktion.

Inden for kryptografien tager man ofte udgangspunkt i at to personer, altid kaldet *Alice* og *Bob*, ønsker at udveksle en besked. En tredje person ved navn *Eve* ønsker så at opsnappe og læse denne besked. (Navnene Alice og Bob er selvfølgelig valgt på grund af deres forbogstaver A og B. Navnet Eve kommer af det engelske ord *eavesdropper*, som er en betegnelse for en person der smuglytter.) Nøgle-distribueringsproblemet kan nu kort skitseres som følger: Hvis Alice og Bob ønsker at udveksle en hemmelig besked, må afsenderen, Alice, kryptere denne. For at Alice kan kryptere beskeden må hun bruge en nøgle – en nøgle som i sig selv er en hemmelighed. Men hvordan får Bob sendt den hemmelige nøgle til Alice, sådan så hun kan sende den hemmelige besked til ham? Kort sagt, for at Alice og Bob kan udveksle en hemmelighed (den krypterede besked) må de allerede dele en hemmelighed (nøglen). Lige meget hvor sikre systemerne beskrevet i forrige afsnit måtte synes at være er de alle underlagt dette problem med distribuering af de hemmelige private nøgler. Efterhånden som kravet om sikkerhed, det vil sige efterspørgslen på sikre kryptosystemer, voksede op igennem de 20. århundrede i takt med den øgede digitalisering, og i øvrigt også den øgede globalisering, blev problemet med distribuering af nøgler mere og mere presserende.

Da telefoner kan blive aflyttet og post kan blive opsnappet er den eneste sikre måde at udveksle private nøgler på at gøre dette fra hånd til hånd, for eksempel ved at de personer som ønsker at udveksle hemmelige beskeder mødes med hinanden. Imidlertid er det ikke altid at personer som ønsker at gøre forretninger med hinanden har mødt hinanden eller har mulighed for

at møde hinanden inden der skal kommunikeres på sikker vis. En tidligere ofte valgt løsning på dette problem var derfor at sende en kurer afsted med nøglen. Var der eksempelvis tale om en oversøisk bankforretning ville banken sende en betroet kurer medbringende en krypteringsnøgle afsted med fly til den pågældende kunde. For en stor bank som foretager mange internationale handler kan man nemt forestille sig hvilken horde af betroede kurerer som denne bank nødvendigvis må have til sin disposition. Det er ikke kun selve distibueringerne af nøgler der på denne vis som kan gå hen og skabe problemer, også omkostningerne forbundet hermed kan nemt blive en belastning. Nogle af de få der langt op i det 20. århundrede var i stand til at holde trit de jævnt stigende omkostninger forbundet med sikker kommunikation var regeringer og militær. Dette skyldtes til dels at de var mere erfarne, men i høj grad også at de havde flere midler til deres rådighed. Problemet for de private virksomheder var derfor åbenlyst: Hvis regeringer og militær havde så store udgifter forbundet med at opretholde sikre kommunikationsveje, hvordan ville situationen så ikke tage sig ud for dem selv?

Men var der da virkelig ingen måde at komme udenom problemet med nøgle-distribution på? I de første tre fjerdedele af det 20. århundrede så det ikke sådan ud – i mere end totusinde år havde distribuering af private nøgler været en uomgængelig forudsætning for etableringen af et kryptosystem. I 1975 ændrede situationen sig imidlertid.

1.3 Offentlig-nøgle kryptering

Problemet med nøgle-distribuering blev i teorien løst i 1975 på Stanford University. Her arbejdede et team bestående af tre unge forskere, Whitfield Diffie, Martin Hellman og Ralph Merkle, sammen om at løse dette ældgamle problem.

Diffie studerede matematik ved MIT i Massachusetts, hvorfra han blev færdig i 1965. Herefter besad han diverse jobs relateret til computersikkerhed og i begyndelsen af 1970'erne havde han udviklet sig til en af de få uafhængige og frittænkende sikkerhedseksperter og kryptografer, som ikke var ansat af enten regeringen eller nogen af de store firmaer på området. Diffie var specielt fascineret og optaget af det begyndende Internet, eller APRANet (Advanced Research Projects Agency Net) som det blev kaldt da det i begyndelsen hørte under det amerikanske forsvar, og han var en af de første der så såvel mulighederne som nogle af problemerne med et sådant stort og internationalt omspændende computernetværk. Allerede tidligt i 1970'erne havde Diffie således indset, at potentialet af det netværk som senere skulle blive til Internettet ville være kraftigt reduceret, hvis ikke man her var i stand til at sende krypterede beskeder. Eksempelvis overvejede han problemet med at handle over dette net: Hvordan kunne en person som ønskede at købe noget sende sine kreditkort-informationer på en sådan måde, at det kun var forhandleren der kunne dechifrere disse? Diffie indså snart, at flaskehalsen i udviklingen og udbredelsen af et sådant netværk (Internettet) ville blive distributionen af nøgler, og det tilmed i et langt større omfang end man

havde oplevet tidligere.

Diffie havde problemer med at finde andre som interesserede sig for dette problem, men i 1974 hørte han ad omveje om Martin Hellman, en professor ved Stanford i Californien. Diffie var en handlingens mand og satte sig derfor for at køre de godt 5000 km til Californien for at møde denne professor, som syntes at dele hans besættelse af nøgle-distribueringsproblemet. Martin Hellman blev noget overrasket den dag i september 1974, da han modtog et telefonopkald fra en vis Whitfield Diffie, som han for det første aldrig havde hørt om, og som for det andet påstod at have kørt tværs over kontinentet for at møde ham. Hellman indvilligede dog i et 30 minutters møde i løbet af hvilket det snart gik op for ham, at han sad overfor en af de mest velinformerede personer inden for kryptografi. Hellman fortæller:

> Jeg havde lovet min kone at komme hjem for at se efter børnene, så han tog med mig hjem og vi spiste middag sammen. Han gik igen omkring midnatstid. Vores personligheder er meget forskellige – han er mere af en modkultur end jeg er – men med tiden gik kultursammenstødet over i en symbiose. Det var sådant et friskt vindpust for mig. At arbejde i et vakuum havde været virkelig hårdt. (Singh; 1999, side 256, oversat fra engelsk)

Ralph Merkle (1952-), Martin Hellman (1945-) og Whitfield Diffie (1944-).

Hellmans kollegaer havde flere gange givet udtryk for, at de ikke forstod han ville arbejde med krytografi, fordi han som kryptograf ved et universitet ville konkurrere med den amerikanske nationale sikkerhedstjeneste NSA (National Security Agency) og deres million-dollar-budget: Hvordan kunne han forestille sig at udvikle noget som de ikke allerede havde lavet, spurgte de. Og hvis han endelig gjorde, ville NSA helt sikkert klassificere det med det samme. Men det tog Hellman sig ikke af, på det område var han ligesom Diffie idealist. Han lod sig drive af sine interesser og delte Diffies opfattelse af, at kryptografi skulle komme alle til gode, ikke kun regeringerne. Hellman havde imidlertid ikke særlig mange penge til sit forskningsprogram og han kunne derfor ikke ansætte Diffie. I stedet blev Diffie indskrevet som studerende ved Stanford og således kunne Hellman og Diffie begynde deres søgen efter en løsning på nøgle-distribueringsproblemet. Med tiden fik de selskab af endnu en forsker, Ralph Merkle. Han var udvandret fra en anden forskningsgruppe, hvor professoren ikke havde nogen sympati for urealistiske drømme om at løse nøgle-distribueringsproblemet. Hellman fortæller:

> Ralph var ligesom os villig til at være et fjols. Og med hensyn til at udvikle original forskning er måden at komme op på toppen på ved at være et fjols, fordi kun fjolser bliver ved med at forsøge. Man har ide nummer 1, man bliver begejstret, og den mislykkes. Så får man ide nummer 2, man bliver begejstret, og den mislykkes. Så får man ide nummer 99, man bliver begejstret, og den mislykkes. Kun et fjols vil igen lade sig begejstre af ide nummer 100, men måske tager det netop 100 ideer før det lykkes. Medmindre man er et stort nok fjols til at blive ved at lade sig begejstre vil man ikke have motivationen, man vil ikke have energien til at stå det igennem. Gud belønner fjolser. (Singh; 1999, side 256, oversat fra engelsk)

Der havde længe fandtes et eksempel på en måde at omgå problemet med nøgle-distribuering på, og Diffie, Hellman og Merkle var bekendt hermed. Lad os forestille os, at Alice ønsker at sende Bob en meget personlig besked og at hun under ingen omstændigheder ønsker at Eve skal kende indholdet af denne. Alice lægger sin besked ned i en stålkasse på hvilken der er plads til to hængelåse. Hun sætter derefter én hængelås på kassen, en lås som kun hun har nøglen til, og sender derefter kassen med postvæsenet til Bob. Når Bob modtager kassen sætter han én til hængelås på, en lås som kun han har nøglen til og sender derefter kassen tilbage til Alice. Alice modtager kassen, piller sin egen hængelås af og sender igen kassen til Bob. Når Bob modtager kassen anden gang er denne nu udelukkende låst med den lås som kun han selv har nøglen til. Bob kan derfor tage denne lås af, åbne kassen og læse Alices besked. Alice og Bob har altså formået at udveksle en hemmelig besked via en offentlig kommunikationsvej uden at de var nødt til at mødes først og udveksle en nøgle og uden at Eve havde mulighed for at opsnappe beskeden.

Metoden ovenfor virker nok for pakker sendt med posten, men den lader sig desværre ikke oversætte til matematik. I systemet ovenfor sker der først to '(ind)krypteringer' og derefter to 'dekrypteringer': Alice sætter sin lås på;

Bob sætter sin lås på; Alice tager sin lås af; Bob tager sin lås af. Det er der fra et matematisk synspunkt sådan set ikke noget mærkeligt i, problemet består i rækkefølgen hvormed kryptering og dekryptering finder sted. Hvis vi beskriver Alices kryptering med den matematiske funktion f, Bobs med den matematiske funktion g og kalder meddelelsen for M, kan de to første skridt altså beskrives ved udtrykket $g(f(M))$. Meddelelsen M kan opnås fra dette udtryk ved først at tage g^{-1}, altså $g^{-1}(g(f(M))) = f(M)$, og dernæst f^{-1}, altså $f^{-1}(f(M)) = M$. Imidlertid er det bare ikke det der sker i eksemplet ovenfor. Her foregår dekrypteringen nemlig i omvendt rækkefølge: Først dekrypterer Alice, f^{-1}, og dernæst Bob, g^{-1}, svarende til at vi får udtrykket $g^{-1}(f^{-1}(g(f(M))))$, et udtryk som matematisk set sjældent giver anledning til M. Generelt gælder der, at den som har indkodet sidst også må afkode først, eller som det gerne hedder 'først på, sidst af'. Lad os se et simpelt eksempel.

Eksempel 1.1
Antag, at vores meddelelse M er et tal og lad funktionerne f og g være givet ved $f(M) = M^3$ og $g(M) = M + 1$. Vi beregner de omvendte funktioner:

$$y = M^3 \Leftrightarrow M = \sqrt[3]{M} \text{ og } y = M + 1 \Leftrightarrow M = y - 1,$$

altså $f^{-1}(y) = \sqrt[3]{y}$ og $g^{-1}(y) = y - 1$. Vi får da

$$g^{-1}(f^{-1}(g(f(M)))) = (\sqrt[3]{((M^3) + 1)}) - 1 = \sqrt[3]{M^3 + 1} - 1,$$

som er forskellig fra M. ◇

En af de få undtagelser på kryptosystemer, hvor dette ikke gælder er rent faktisk Cæsar-kryptering (se opgave 7). Men som vi allerede har set er Cæsar-kryptering et alt andet end sikkert kryptosystem. Generelt regner man med at sikre kryptosystemer opfylder reglen om 'først på, sidst af'.

Hellman og Merkle var mest optaget af at finde en sikker metode til udveksling af nøgler mens Diffie var optaget af at følge en anden vej, den vej som skulle vise sig at føre til hvad der i dag er kendt som *offentlig-nøgle kryptering*. Diffie genkalder sig den dag i 1975, hvor han fik ideen til offentlig-nøgle kryptering således:

> Jeg gik nedenunder for at få en Coke og glemte næsten helt ideen. Jeg huskede, at jeg havde haft tænkt på et eller andet interessant, men jeg kunne ikke genkalde, hvad det var. Så kom det tilbage i et rigtigt adrenalinsus af ophidselse. For første gang mens jeg havde arbejdet med kryptografi var jeg rent faktisk klar over at jeg havde opdaget noget rigtig værdifuldt. Alt hvad jeg havde opdaget op til dette tidspunkt forekom mig nu kun at være teknikaliteter. (Singh; 1999, side 268, oversat fra engelsk)

Men hvad var det så for en ide Diffie havde fået? Lad os for et kort øjeblik lige genkalde os, hvad det er som er essensen af privat-nøgle eller symmetrisk kryptering. I et privat-nøgle kryptosystem besidder afsender og modtager

en ækvivalent viden, da nøglerne til (ind)kryptering og dekryptering jo i bund og grund er den samme – systemet er altså symmetrisk. Hvad Diffie derimod havde tænkt var: Hvad nu hvis nøglerne til (ind)kryptering og dekryptering *ikke* er den samme? Hvad nu hvis systemet ikke er symmetrisk, men *asymmetrisk*? I et asymmetrisk kryptosystem kan Bob, hvis han kender (ind)krypteringsnøglen, kryptere en besked til Alice. Men han kan ikke selv dekryptere den, det er kun Alice, som kender dekrypteringsnøglen, som kan det. Hvis vi bliver i analogien med kassen og hængelåsene er der altså tale om, at Alice stiller en masse hængelåse til rådighed som kun hun har nøglerne til, eksempelvis ved at bede postkontoret om at opbevare disse. Bob kan derefter gå ned på postkontoret, bede om 'Alice-hængelåsen', sætte denne på sin kasse og derefter sende kassen indeholdende den hemmelige besked til Alice. Bob kan ikke selv åbne kassen igen, det er kun Alice, da hun alene har nøglen til 'Alice-hængelåsen'. Tilmed er det ikke kun Bob som kan sende beskeder sikkert til Alice på denne måde, også Cecilie, David og Elisabeth kan gå ned på postkontoret og bede om 'Alice-hængelåsen'. Hvis Alice derimod ønsker at svare på Bobs besked, må hun gå ned på postkontoret og bede om 'Bob-hængelåsen'. Pointen her er, at (ind)krypteringsnøglen, Alice-hængelåsen eller Bob-hængelåsen afhængig af hvem der sender til hvem, er offentligt tilgængelig og ikke hemmelig. Alle, heriblandt Eve, kan få fat i denne offentlige nøgle til (ind)kryptering og der er ingen fare forbundet dermed, for man kan kun kryptere beskeden, ikke dekryptere den igen. Medmindre selvfølgelig man som Alice er i besiddelse af den private (dekrypterings)nøgle som er i stand til at åbne hængelåsen. Et system der fungerede som dette ville en gang for alle løse nøgle-distribueringsproblemet. Med offentlig-nøgle kryptering skulle Bob blot kigge i et eller andet register, for eksempel lokaliseret i en telefonbog eller på nettet, finde værdien svarede til Alices offentlige nøgle, kryptere beskeden og sende den afsted. Situationen er skitseret på figur 1.2. (Diffies og Hellmans oprindelige figur fra 1976 er gengivet på forsiden af undervisningsmaterialet (Diffie & Hellman; 1976, side 647)).

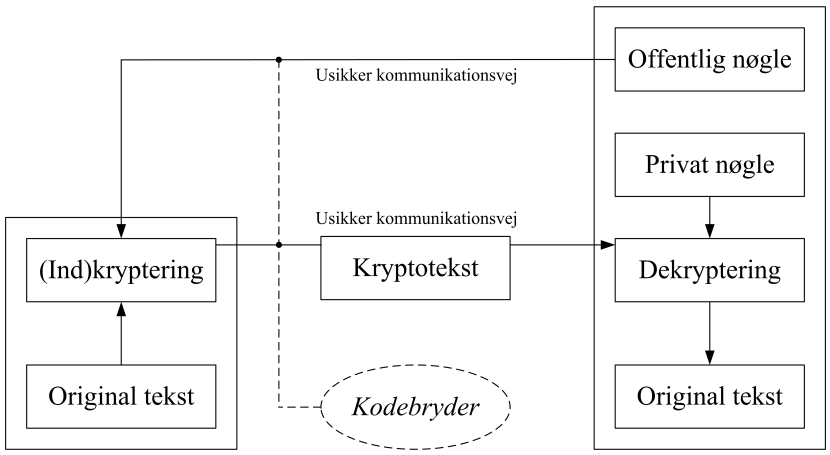
Men ét var imidlertid, at Diffie havde fået ideen til et asymmetrisk kryptosystem og indset at det var en teoretisk mulighed. Noget andet var at finde en matematisk funktion som opfyldte kravene og kunne udføre jobbet. Det var klart at der måtte være tale om en såkaldt *envejsfunktion*, hvilket kan 'defineres' på følgende vis:

Definition 1.2
En funktion f siges at være en envejsfunktion*, hvis det for ethvert x i dens definitionsmængde er nemt at beregne den tilsvarende værdi $f(x)$, men det for enhver værdi $y = f(x)$ i f's værdimængde for alle praktiske formål er umuligt at beregne $f^{-1}(y) = x$.*

Bemærk, at der her ikke i gængs forstand er tale om en matematisk definition, idet det er ikke er helt klart hvad formuleringen 'for alle praktiske formål' helt præcist dækker over. Tilmed er betegnelsen en 'envejsfunktion' måske heller ikke den mest heldige, da jo alle funktioner kun går én vej. Men historisk set er det altså denne betegnelse og denne definition som Diffie og Hellman havde til deres rådighed. Med udgangspunkt i

'definitionen' er der således ikke tale om, at den omvendte, f^{-1}, ikke eksisterer, men derimod om at det vil være alt for besværligt at bestemme den. En funktion, hvorom der gælder at man kan beregne $f(x)$ på få sekunder, men hvor det vil tage en computer en million år at beregne $f^{-1}(y)$ vil være en envejsfunktion. Med andre ord kan vi sige, at envejsfunktioners omvendte ikke i teorien er uberegnelige, men at de er det i praksis. Funktioner der ikke er envejsfunktioner kaldes *tovejsfunktioner*. Diffies ide til et kryptosystem måtte altså bygge på en envejsfunktion f, hvor det for alle praktiske formål ville være umuligt udelukkende udfra kendskab til funktionen f (den offentlige nøgle) såvel som dens funktionsværdier $y = f(M)$ at bestemme M'erne. Og samtidig en envejsfunktion, hvor man med et stykke speciel information (den private nøgle) ville være i stand til at bestemme M udfra $y = f(M)$. Men hvilken envejsfunktion besad disse egenskaber? Lige meget hvor meget Diffie og Hellman søgte kunne de ikke finde en funktion som opfyldte kravene.

Selv om de ikke kunne finde en envejsfunktion som passede på kravene til offentlig-nøgle kryptering bar deres arbejde alligevel i nogen grad frugt. I foråret 1976 fandt Hellman en matematisk envejsfunktion, og en måde at anvende denne på, som kunne bruges til hemmelig nøgleudveksling ad en offentlig (usikker) kommunikationsvej. Funktionen passede ikke på kravene stillet til Diffies asymmetriske kryptering, men den løste det ældgamle problem med nøgle-distribution. Metoden er i dag kendt som *Diffie-Hellman-Merkle*



Figur 1.2 Asymmetrisk eller offentlig-nøgle kryptering: Modtageren har i forvejen genereret en offentlig nøgle og stillet denne til rådighed for afsenderen via en usikker kommunikationsvej. Afsenderen anvender denne offentlige nøgle til at (ind)kryptere sin originale tekst og får derved kryptoteksten. Denne sendes, ligesom den offentlige nøgle blev det, via en usikker kommunikationsvej. En eventuel kodebryder kan derfor opsnappe såvel kryptoteksten som den offentlige nøgle. Modtageren dekrypterer kryptoteksten med sin egen private nøgle, hvilket giver den originale tekst.

nøgleudveksling. Den envejsfunktion som indgår i udvekslingen kræver en matematisk viden som vi endnu ikke har udfoldet i dette undervisningsmateriale, så forklaringen af denne vil blive udsat til senere (opgave 72), men ideen i udvekslingen kan vi godt forklare her. Denne går ud på, at Alice og Bob ad en offentlig kommunikationsvej, for eksempel telefonen, først bliver enige om nogle *parameterværdier* for funktionen, hvilket vil sige at de aftaler dennes præcise udseende. Har vi eksempelvis givet en lineær funktion $f(x) = sx+t$ er der jo i virkeligheden tale om uendelig mange forskellige funktioner afhængig af værdierne af s og t. At blive enige om nogle parameterværdier for denne funktion vil sige, at man bliver enige om nogle helt konkrete talværdier for s og t, for eksempel $s = 3$ og $t = 7$, hvilket fastlægger funktionen fuldstændigt til $f(x) = 3x + 7$. Når Alice og Bob således har fastlagt deres funktion gennem valget af parameterværdier vælger de hver især et hemmeligt tal, henholdsvis a og b, og plotter dette ind i envejsfunktionen med de aftalte parameterværdier. Dette giver dem funktionsværdierne α og β. Alice sender nu sin værdi α til Bob ad den offentlige kommunikationsvej, og Bob sender sin værdi β til Alice ad samme vej. Den specielle envejsfunktion som Hellman fandt fungerer nu på den måde, at når Alice sætter Bobs β ind i denne får hun en talværdi γ, og når Bob sætter Alices α ind i funktionen får han den samme talværdi γ. Alice og Bob har nu begge den samme private nøgle γ og de har ikke skulle mødes for at udveksle den. Samtidig kan Eve ikke, på grund af envejsfunktionens specielle natur, på nogen måde beregne γ, heller ikke selvom hun opsnapper både parameterværdierne til envejsfunktionen og funktionsværdierne α og β. Den udvekslede private nøgle γ kan derefter bruges i et mellem Alice og Bob aftalt symmetrisk kryptosystem.

Hellmans ide til offentlig-nøgle udveksling løser således nøgle-distribueringsproblemet for et symmetrisk kryptosystem. Imidlertid er udvekslingen stadig langt fra optimal, idet der nødvendigvis må finde en kommunikation sted inden den krypterede meddelelse kan sendes. Antag, at Alice og Bob bor i to forskellige lande med flere tidszoner imellem sig, og at Alice ønsker at sende en hemmelig besked til Bob. Alice må først ringe til Bob og aftale parametrene til envejsfunktionen. Når dette er gjort skal de bruge denne på deres valgte tal a og b for at få α og β. For at udveksle disse værdier skal de igen ringe til hinanden. Med flere tidszoner imellem sig og dermed forskellige sove- og arbejdstider kan man nemt forestille sig situationer, hvor en sådan udveksling til tage adskillige timer eller måske endda dage. Så lang ventetid er selvfølgelig en bet, i flere tilfælde vil det måske endda være for sent for Bob først at modtage beskeden dagen efter. I forretningstransaktioner, hvor beskeden måske kunne være; 'køb de og de aktier NU!' eller i en krigssituation hvor beskeden måske er; 'angrib fjenden NU!', kan en sådan forsinkelse tilligemed være katastrofal for de involverede parter.

Ovenstående situation gør sig imidlertid ikke gældende for asymmetriske kryptosystemer. Her benytter man blot den offentligt tilgængelige nøgle og efter (ind)kryptering af sin besked kan man sende denne med det samme. Offentlig-nøgle kryptering var altså stadig at foretrække frem for Diffie-Hellman-Merkle nøgleudveksling. Men problemet med envejsfunktionen til offentlig-nøgle kryptering lod ikke til at lade sig løse. Efter yderligere forgæves

søgen valgte Diffie og Hellman at offentliggøre deres ideer. Dette gjorde de i november 1976 i artiklen *New Directions in Cryptography*. Diffie og Hellman beskriver i begyndelsen af denne artikel deres motivation for at beskæftige sig med disse nye 'trends' i kryptografi på følgende vis:

> Vi står i dag på tærsklen til en revolution inden for kryptografi. [...] Udviklingen af computerkontrollerede kommunikationsnetværk lover en ubesværet og billig kontakt mellem folk eller computere på hver sin side af Jorden, dermed erstattende fortrinsvist post og mange afstikkere med telekommunikationer. For mange applikationer må disse kontakter være sikret både imod smuglyttere og tilførsel af illegitime meddelelser. Som tingene ser ud nu halter løsningen af disse sikkerhedsproblemer langt efter andre områder af kommunikationsteknologi. Den nuværende kryptografi er ikke i stand til at imødekomme kravene, forstået på den måde at brugen heraf vil påtvinge systemets brugere så alvorlige besværligheder, at det vil eliminere mange af fordelene [...] Det bedst kendte kryptografiske problem er det omhandlende hemmeligholdelse: ved brug af kryptografi at forhindre en uautoriseret udtrækning af information fra kommunikationer ad en usikker kommunikationsvej. På nuværende tidspunkt er det imidlertid nødvendigt for de kommunikerende parter at dele en nøgle som ikke kendes af andre. Dette ordnes ved at sende nøglen i forvejen ad en sikker kommunikationsvej såsom med privat kurer eller med anbefalet post. [...] Omkostningerne og tidsforsinkelserne forårsaget af dette problem med nøgle-distribution udgør en markant barriere for overførslen af information mellem virksomheder og store computernetværk. (Diffie & Hellman; 1976, side 644, oversat fra engelsk)

Udover ideen til offentlig-nøgle kryptering beskriver Diffie og Hellman i artiklen også, hvorledes man, hvis man først har et offentlig-nøgle system, kan løse problemet med *autentifikation* – det digitalt ækvivalente til en skreven underskrift. Løsningen af dette problem har i høj grad sin relevans i forbindelse med brugen af kreditkort. Med hensyn til offentlig-nøgle kryptering så giver Diffie og Hellman en grundig gennemgang af de krav der må stilles til en matematisk funktion for at denne kan udføre jobbet, samtidig med at de erkender, at de ikke selv har været i stand til at finde en der passer til beskrivelsen. De afslutter artiklen med følgende appel til deres kryptografikollegaer:

> Vi håber at dette vil inspirere andre til at arbejde inden for dette fascinerende område, hvor deltagelse er blevet modvirket i den nærmeste fortid af et næsten totalt regeringsmonopol. (Diffie & Hellman; 1976, side 653, oversat fra engelsk)

Diffie og Hellman håbede ikke forgæves. Allerede året efter fandt tre andre unge forskere ved Diffies gamle universitet, MIT, en matematisk envejsfunktion som opfyldte Diffies og Hellmans krav. Det offentlig-nøgle kryptosystem som bygger på den funktion de fandt kendes i dag som *RSA* efter opfindernes initialer: Rivest, Shamir og Adleman. Motivationen for de tre forskere fra MIT synes at være næsten identisk og mindst lige så fremsynet som den

af forskere fra Stanford. Forskerne fra MIT skriver således i indledningen til deres artikel:

> Den 'elektroniske posts' ære kan snart være over os. Vi må derfor sikre os at to vigtige egenskaber ved det nuværende system med 'papirpost' forbliver bevaret: (a) meddelelser må være *private* og (b) meddelelser må være *underskrevet*. (Rivest et al.; 1978, side 1, oversat fra engelsk)

RSAs specielle envejsfunktion tilhører det område af matematikken der kendes som *talteori* – en omfattende og ældgammel matematisk disciplin. Før vi således kan give en fyldestgørende beskrivelse af, hvordan envejsfunktionen i RSA opfylder Diffies og Hellmans krav til offentlig-nøgle systemer bliver vi nødt til at have noget matematik på banen. Dette foregår i kapitel 2 og kapitel 3 og beskrivelsen af RSA følger så i kapitel 4. Ydermere er vi nødt til at få en ide om, hvad algoritmer inden for matematikken er, da RSA er et eksempel på en sådan og da der også inden for talteorien selv findes algoritmer. Så det gør vi nu.

1.4 Lidt om algoritmer

RSA er som sagt en algoritme. Det vil sige, at man for at (ind)kryptere og dekryptere følger nogle helt bestemte og fastlagte procedurer. I eksemplet fra afsnit 1.1 med Cæsar-kryptering var den fastlagte procedure for kryptering ganske enkelt:

1. Udskift hvert bogstav i beskeden med det bogstav der står tre pladser længere fremme i alfabetet.

Man må selvfølgelig tilføje, at hvis der er tale om et af de tre sidste bogstaver i alfabetet så tæller man videre fra begyndelsen af alfabetet. Proceduren for dekryptering lyder:

2. Udskift hvert bogstav i beskeden med det bogstav der står tre pladser tidligere i alfabetet.

Igen må man tilføje, at hvis der er tale om et af de tre første bogstaver i alfabetet så tæller man videre bagfra i alfabetet. Der er altså tale om to simple procedurer som tilsammen giver os en algoritme for udførelsen af Cæsar-kryptering.

Selve navnet 'algoritme' er en forvanskning af navnet al-Khowarizmi. Abu Ja'far Mohammed Ibn Musa al-Khowarizmi (ca. 780-850) var astronom og matematiker i Bagdad og det fra hans bog *Kitab al-jabr w'al muquabala* at navnet 'algebra' stammer – al-jabr blev til algebra. Bogen omhandler aritmetiske operationer med hinduistiske taltegn, hvilket vil sige de tal vi i dag bruger. (Godt nok omtaler vi gerne vores tal som arabertal, men faktisk er der tale om de hinduistiske taltegn. Arabernes tal ser ganske anderledes ud.) Gennem den latinske forvanskning af al-Khowarizmis navn kom algoritme med tiden til at betyde aritmetisk operation med hinduistiske taltegn og senere det som vi i dag forstår ved en algoritme. For at være helt på det rene med, hvad det er vi i dag forstår ved begrebet algoritme skal vi give følgende definition.

Definition 1.3
En algoritme *er en endelig mængde af præcise instruktioner for udførelsen af en beregning eller løsningen af et problem.*

Generelt set opfylder algoritmer gerne en række egenskaber, eller man er i hvert fald interesseret i at de gør det, da brugbarheden af dem ellers kan være diskutabel. Disse egenskaber er som følger:

1. *Inddata*: En algoritme modtager værdier fra en nærmere specificeret mængde af inddata.
2. *Uddata*: Fra hver mængde af inddata giver algoritmen uddata fra en nærmere specificeret mængde af sådanne. Uddata-værdierne er løsningerne til problemet.
3. *Præcision*: Skridtene af en algoritme må være præcist defineret.
4. *Korrekthed*: En algoritme må producere de korrekte uddata-værdier for hver mængde af inddata-værdier.
5. *Terminering*: En algoritme må producere det ønskede uddata i løbet af et endeligt, omend eventuelt stort, antal skridt for en hvilken som helst mængde af inddata.
6. *Effektivitet*: Det skal være muligt at udføre hvert skridt i algoritmen nøjagtigt som tiltænkt og inden for en endelig tidsperiode.
7. *Generalitet*: Algoritmen bør kunne anvendes for alle problemer af den ønskede form, ikke kun for en speciel mængde af inddata-værdier.

Lad os eksemplificere dette med udgangspunkt i Cæsar-kryptering.

Eksempel 1.4
For den ovenstående algoritme for Cæsar-kryptering udgør den besked der skal krypteres vores inddata-værdier. Den nærmere specificerede mængde, hvorfra inddata-værdierne kommer er vores alfabet bestående af 29 bogstaver. Algoritmen giver løsningen, det vil sige den krypterede besked, som uddata-værdier ligeledes bestående af bogstaver fra alfabetet (den specificerede mængde). Skridtene i algoritmen er præcist defineret; før afsendelse foretages kryptering, efter modtagelse foretages dekryptering. I hvert af disse skridt udskiftes bogstaverne løbende med henholdsvis bogstaverne tre pladser længere fremme eller tre pladser længere tilbage i alfabetet. Algoritmen giver en korrekt kryptering, hvis den er implementeret i overenstemmelse med forskrifterne, og i så fald også en korrekt dekryptering. Hvis ellers beskeden er endelig kan algoritmen også udføres i et endeligt antal skridt; når vi når sidste bogstav i beskeden terminerer algoritmen. Og i så fald kan algoritmen også afsluttes inden for en endelig tidsperiode. Med hensyn til generalitet, så fungerer algoritmen på samtlige kombinationer af inddata fra alfabetet.

Algoritmen kan faktisk også være generel på anden vis, idet vi kan generalisere værdien 3 til at være k, hvor k er mindre end eller lig antallet af symboler i alfabetet. Men det er ikke denne form for generalitet som den syvende egenskab for algoritmer hentyder til. ◇

En af de ting der muliggjorde en realisering af RSA-kryptosystemet var tilstedeværelsen af computere. Og med computernes indtog har netop algoritmer fået en langt mere fremtrædende rolle i vores samfund og hverdag end de har haft tidligere. Som et meget oplagt eksempel kan selvfølgelig nævnes de programmer som vi hver især kører på vores pc'er eller mac. Når vi for eksempel ønsker at få fremvist indholdet af en mappe på vores computer kan vi vælge hvorledes dette skal foregå; skal filerne vises i alfabetisk rækkefølge, skal de vises i overensstemmelse med deres filtype, hvornår de er blevet oprettet eller noget fjerde? Hver gang vi foretager et sådant valg anvender computeren et program som indeholder en algoritme til at sortere filerne. Rent faktisk er sorteringsalgoritmer inden for datalogien et kæmpe område, hvor det gælder om at vide hvilke algoritmer der egner sig bedst til hvilke opgaver. Nogle algoritmer er nemlig hurtigere til at gå fra én sortering til en anden end andre, og som programmør, software-udvikler eller måske endda software-udbyder er man selvfølgelig interesseret i at anvende så hurtige procedurer som muligt og eventuelt også procedurer som anvender så lidt hukommelse (plads) som muligt. Algoritmers hurtighed, også kaldet deres kompleksitet, skal vi imidlertid ikke berøre yderligere i dette undervisningsmateriale, idet dette emne i højere grad hører datalogien til end matematikken – og det er matematikken som er vores omdrejningspunkt her.

En af de første algoritmer vi kender til i historien er den der i dag kendes som Euklids algoritme. Denne algoritme udgør i dag en hjørnesten i talteori. Vi skal bruge algoritmen flere gange i de følgende kapitler, såvel i udregninger som i beviser, og ikke mindst i forbindelse med RSA. Euklids algoritme vil blive beskrevet i det følgende kapitel.

1.5 Opgaver

Opgave 1
Forklar begreberne: kryptering, dekryptering, kryptotekst, kryptosystem, kryptograf, kryptoanalyse, kodebryder, sikker kommunikationsvej, usikker kommunikationsvej.

Opgave 2
Forklar begreberne: privat-nøgle kryptering, nøgle-distribueringsproblemet, offentlig-nøgle udveksling, offentlig-nøgle kryptering.

Opgave 3
Krypter beskeden `OGSÅ DU MIN SØN BRUTUS` med Cæsar-kryptering.

Opgave 4
Anvend frekvensanalyse til at bryde beskeden `ZÆMMÆ ÆK DHKKÆDM`.

Opgave 5
Lad $f(x) = x - 7$, $g(x) = x^5 + 1$, $h(x) = e^x$, $l(x) = \ln(x + 3)$ være funktioner med definitionsmængde og værdimængde lig $\mathbb{R}$ (de reelle tal). Bestem disse funktioners omvendte.

Opgave 6
Et eksempel på en privat-nøgle kryptering som kan være umulig at bryde er den såkaldte *bogkode*. I en bogkode udgør en skrevet tekst den private nøgle. Hvert ord i teksten er nummereret fortløbende og nummeret angiver det første bogstav i ordet (punktum, komma, etc. ignoreres). En besked krypteres så ved at finde samme bogstav i teksten og i stedet for bogstavet skrive nummeret. Hvis vi anvender citatet på side 15 fra Diffies og Hellmans artikel får vi følgende:

> [1]Vi [2]står [3]i [4]dag [5]på [6]tærsklen [7]til [8]en [9]revolution [10]inden [11]for [12]kryptografi. [...] [13]Udviklingen [14]af [15]computerkontrollerede [16]kommunikationsnetværk [17]lover [18]en [19]ubesværet [20]og [21]billig [22]kontakt...

Vi kan så (ind)kryptere beskeden `DIFFIE` til for eksempel `4,3,11,11,10,18`.

a. Skriv en tekst til din sidemand på en ti-femten ord og (ind)krypter den ved hjælp af *hele* Diffie og Hellman citatet på side 15.
b. Du og din sidemand udveksler nu krypterede beskeder og dekrypterer hver især hinandens.
c. Hvad skal man tage højde for når man vælger tekst til brug i en bogkode?
d. Hvad kan man gøre med hensyn til valg af tekst for at gøre sin bogkode så godt som helt sikker mod angreb?

Opgave 7
Cæsar-(ind)kryptering kan beskrives ved funktionen $f(x) = x+3$. Redegør generelt for at princippet 'først på, sidst af' ikke gælder i tilfældet med Cæsar-kryptering ved at se på de to funktioner til (ind)kryptering givet ved $f(x) = x + b$ og $g(x) = x + d$.

Opgave 8
Hvad hvis funktionerne til (ind)kryptering er givet ved $f(x) = ax + b$ og $g(x) = cx + d$, gælder princippet 'først på, sidst af' da?

Opgave 9
Cæsar-kryptering er et eksempel på kryptering ved *substitution*, altså at man substituerer et tegn for et andet i overenstemmelse med en given regel. En anden form for kryptering er kryptering ved *permutation*. Her ombytter man tegnene i en given besked som for eksempel her,

`OGSÅ DU MIN SØN BRUTUS` → `GOÅS UD IMS NNØ RBTUSU`,

hvor første og andet tegn ombyttes, tredje og fjerde tegn ombyttes, og så videre.

a. Bryd den permuterede besked: `EDØR RE RESOR ELLA EKKI`.
b. Bryd den permuterede besked: `MAGLEM TSO GULRET`.
c. Opskriv en besked til din sidemand og krypter denne ved permutation. Lad din sidemand gøre det samme. Byt derefter krypterede beskeder og forsøg at bryde hinandens krypteringer.

ABCDEFGHIJKLMNOPQRSTUVWXYZÆØÅ
BCDEFGHIJKLMNOPQRSTUVWXYZÆØÅA
CDEFGHIJKLMNOPQRSTUVWXYZÆØÅAB
DEFGHIJKLMNOPQRSTUVWXYZÆØÅABC
EFGHIJKLMNOPQRSTUVWXYZÆØÅABCD
FGHIJKLMNOPQRSTUVWXYZÆØÅABCDE

Tabel 1.1 De seks første substitutionsalfabeter af Vigenère-koden.

Opgave 10
Tabel 1.1 angiver de seks første substitutionsalfabeter af Vigenère-koden. Måden at angive en nøgle på i dette kryptosystem var ved at danne et ord ud forskellige bogstaver. For eksempel vil ordet `BAD` angive, at første bogstav i den originale tekst skal substitueres med bogstavet under dette i den række der begynder med `B`, andet bogstav i beskeden med bogstavet i den række der begynder med `A`, og tredje bogstav med den tilsvarende i rækken som begynder med `D`, og derefter begynder man forfra. Eksempelvis vil vi have, at

$$\texttt{VIGENERE} \longrightarrow \texttt{WIJFNHSE}.$$

a. Krypter beskeden `VIGENERE` anvendende nøglen `ABE`.
b. Krypter beskeden `CHARLES BABBAGE` anvendende nøglen `FED`.
c. Udvid tabel 1.1 til at omfatte samtlige 29 bogstaver i alfabetet og dekrypter dernæst beskeden `PIGTWJSTF LBDRVJB DSCZQZB` ved brug af nøglen `KRYPTOS`.

Opgave 11
Hvilke af de syv egenskaber for algoritmer vil du karakterisere som værende de vigtigste? Hvorfor netop disse?

2 Elementær talteori

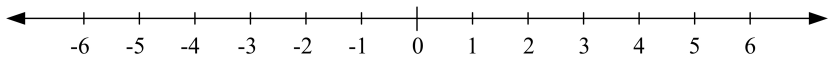
Den elementære talteori som vi skal beskæftige os med i dette kapitel kan for en stor dels vedkommende spores helt tilbage til antikkens Grækenland. I har måske hørt om matematikeren Euklid som omkring år 300 f.v.t. havde sit virke i Alexandria, hvor han forfattede bøgerne kendt som Euklids *Elementer*. Elementerne omfatter i alt tretten bøger, hvoraf de fleste omhandler geometri. Men tre af bøgerne omfatter også 'elementer' af det som vi i dag vil regne for talteori, nærmere bestemt er der tale om bog VII, bog VIII og bog IX. Mange af de begreber som vi skal møde i dette kapitel så som primtal, sammensat tal, indbyrdes primisk, største fællesdivisor og mindste fælles multiplum kan spores tilbage til Elementerne. Dertil kommer Euklids sætning om antallet af primtal samt Euklids algoritme som vi også skal se i dette kapitel.

Når Euklid, og grækerne dengang, talte om *tal* så mente de de naturlige tal, $\mathbb{N} = \{1, 2, 3, \ldots\}$, og faktisk regnede de ikke engang tallet 1 med. Dette skyldtes, at tallet 1 besad en særstatus af at repræsentere én *enhed* og det var udfra denne de øvrige tal blev defineret. De første to definitioner i Euklids bog VII lyder således:

> 1. En *enhed* er en sådan i kraft af hvilken hver af de ting der eksisterer kaldes én [tallet 1].
> 2. Et *tal* er en mængde sammensat af enheder. (Euclid; 1956, vol. 2, side 277)

Euklid (ca. 325 - ca. 265 f.v.t.)

Ikke meget vides om Euklid af Alexandria som person udover at han underviste i Alexandria i Egypten. Det menes dog sikkert, at han har levet senere end de græske matematikere Eudoxus (408 - 355 f.v.t.) og Theaetetus (ca. 417 - ca. 369 f.v.t.), idet han fremlægger og fortolker disses arbejder, men før matematikeren Archimedes (287 - 212 f.v.t.). Ifølge den græske filosof Proklos (411-485) var Euklid platonist af overbevisning. Euklid er kendt for sine *Elementer*, et stort matematisk værk opdelt i tretten bøger, hvori der behandles store dele af datidens kendte geometri og talteori. Det siges, at efter Biblen er Euklids *Elementer* muligvis det mest oversatte, publicerede og studerede af alle værker i den vestlige verden. Elementerne er også at regne for den primære kilde inden for geometrisk ræsonneren (sætninger og metoder), om ikke andet så indtil fremkomsten af ikke-euklidisk geometri i 1800-tallet. Helt op i det tyvende århundrede har læsning af Elementerne også været en obligatorisk del af de fleste matematikuddannelser, herunder de gymnasiale.



Figur 2.1 De hele tal, $\mathbb{Z}$.

Vi skal imidlertid i det følgende udvide vores opfattelse af tal en smule i forhold til Euklids. Vi vil som vi normalt gør regne 1 for et tal og tilmed vil vi ikke kun begrænse os til de naturlige tal, men derimod betragte de hele tal, $\mathbb{Z}$, (se figur 2.1), hvilket er det man gør i moderne talteori. Den oplagte årsag til at grækerne ikke betragtede de hele tal er at de ikke kendte til negative tal eller tallet nul for den sags skyld. Disse blev først introduceret langt senere i historien. Selvom de resultater som findes i Euklids *Elementer* således oprindeligt kun er tænkt at gælde for $\mathbb{N}\setminus\{1\}$ gælder de (oftest) også for de resterende hele tal. I og med at den følgende præsentation af den elementære talteori er en moderne præsentation skal vi som sagt udvikle denne for heltal ($\mathbb{Z}$).

2.1 Division og største fællesdivisor

Hvad vil det sige, at et tal går op i et andet tal? Når man kun arbejder med heltal, som vi skal her, er definitionen af 'at gå op i' en smule anderledes end vi normalt er vant til, idet et heltal kun siges at gå op i et andet heltal, hvis resultatet bliver et tredje heltal. Man accepterer altså hverken brøker eller decimaltal som resultat. I dette afsnit skal vi se, hvordan man med udgangspunkt i en sådan definition af at 'gå op i' kan vise flere interessante egenskaber ved heltal og ikke mindst ved de specielle heltal der kendes som primtal. Men først definitionen.[1]

Definition 2.1: $a \mid b$
Lad a, b og c være heltal med $a \neq 0$. Vi siger, at a går op i *b, og skriver $a \mid b$, hvis der findes et heltal c således, at $ac = b$.*

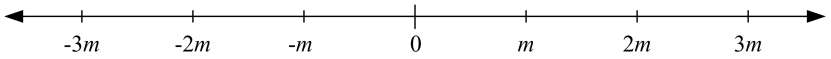
Når $a \mid b$ siges a at være en *faktor* eller en *divisor* i b og b et *multiplum* af a. Hvis a *ikke* er en faktor i b skriver vi $a \nmid b$. Lad os se et eksempel.

Eksempel 2.2
Hvis $a = 4$ og $b = 20$ har vi $4 \mid 20$ da $4 \cdot 5 = 20$, det vil sige $c = 5$. Vi siger altså, at 4 går op i 20, at 4 er en faktor i 20 eller at 20 er et multiplum af 4.

Kigger vi derimod på $a = 3$ og $b = 20$ ser vi, at $3 \nmid 20$ da der ikke findes noget heltal c som ganget med 3 giver 20 (der gælder jo $20/3 = 6\frac{2}{3}$). $\diamond$

En af de sætninger man med udgangspunkt i ovenstående definition kan vise er den følgende.

[1] Væsentlige dele af den matematiske fremstilling i dette kapitel er baseret på (Rosen; 2003) og (Biggs; 1989).



Figur 2.2 De heltal som det positive heltal m går op i.

Sætning 2.3
Lad a, b og c være heltal. Der gælder da følgende:

i. Hvis $a \mid b$ og $a \mid c$, så vil $a \mid (b+c)$.

ii. Hvis $a \mid b$, så gælder der for alle heltal c, at $a \mid bc$.

iii. Hvis $a \mid b$ og $b \mid c$ så gælder, at $a \mid c$.

Bevis
Vi begynder med (*i*): Antag, at $a \mid b$ og $a \mid c$. Ifølge definition 2.1 findes der da heltal s og t således, at $as = b$ og $at = c$. Der gælder da, at $b + c = as + at = a(s + t)$, hvilket jo netop medfører, at $a \mid (b + c)$.

For at bevise (*ii*) antager vi, at $a \mid b$. Det betyder, at der findes et heltal s, således at $as = b$. Vi forlænger nu med et heltal c på begge sider af denne lighed og får $asc = bc$ som vi skriver som $a(cs) = bc$. Altså haves at $a \mid bc$, og da c kan være et hvilket som helst heltal gælder sætningen for alle heltal c.

Og til slut (*iii*): Antag, at $a \mid b$ og $b \mid c$. Det vil sige, der findes heltal s og t således, at $b = as$ og $c = bt$. Vi kigger da på udtrykket $a(st)$. Dette er lig bt, som igen er lig c. Altså $a(st) = bt = c$, hvorfor der må gælde, at $a \mid c$. □

Eksempel 2.4
For at illustrere (*i*) kan vi se på $a = 213$, $b = 1704$ og $c = 2769$. Da $213 \mid 1704$ ($213 \cdot 8 = 1704$) og $213 \mid 2769$ ($213 \cdot 13 = 2769$), har vi ifølge sætningen at $213 \mid (1704 + 2769) = 4473$. (Check selv!)

Når $a = 213$ og $b = 1704$ og vi ved at $213 \mid 1704$, så gælder der ifølge (*ii*), at 213 vil gå op i produktet af et hvilket som helst heltal c ganget med 1704. Helt præcist vil det gå op $213 \cdot c$ gange.

Et eksempel på (*iii*) kan være $a = 213$, $b = 1704$ og $c = 11928$. Da $213 \mid 1704$ og $1704 \mid 11928$ ($1704 \cdot 7 = 11928$) gælder ifølge sætningen, at 213 går op i 11928. Hvor mange gange 213 går op er let at se, for da 213 går 8 gange op i 1704 og 1704 går 7 gange op i 11928 vil 213 gå $8 \cdot 7 = 56$ gange op i 11928. ◇

En sætning der mere eller mindre helt naturligt falder ud af en anden sætning eller er en direkte konsekvens af en sætning kendes som et *korollar*, eller med et mere jævnt navn en følgesætning. Sætning 2.3 har et sådant korollar.

Korollar 2.5
Hvis a, b og c er heltal og $a \mid b$ og $a \mid c$ så gælder, at $a \mid mb + nc$ for to vilkårlige heltal m og n.

Bevis
Af sætning 2.3 (*ii*) følger, at $a \mid mb$ og $a \mid nc$. Af (*i*) følger, at $a \mid mb + nc$. □

Vi skal nu definere et centralt begreb, nemlig det af største fællesdivisor.

Definition 2.6: Største fællesdivisor
Lad a og b være heltal således, at de ikke begge er nul. Det største heltal d således, at $d \mid a$ og $d \mid b$, kaldes den største fællesdivisor *af a og b og skrives* $\text{sfd}(a, b)$.

At det giver mening, at tale om et sådant bestemt heltal d følger netop af, at a og b ikke begge er nul. Havde de begge været nul, havde vi kunne vælge et vilkårligt største heltal d, da alle tal jo går op i nul. Bemærk endvidere, at hvis $a = 0$ vil $d = b$ og hvis $b = 0$ vil $d = a$.

Eksempel 2.7
Vi har givet de to heltal 24 og 36 og skal finde $\text{sfd}(24, 36)$. En måde at gøre det på er ved at opskrive to mængder, en med divisorerne i 24 og en med divisorerne i 36 og dernæst identificere den største divisor der optræder i begge mængder. Hvis vi kalder mængden af divisorer i 24 for A og mængden af divisorer i 36 for B har vi

$$A = \{1, 2, 3, 4, 6, 8, 12, 24\} \quad \text{og} \quad B = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}.$$

Vi kan nu opskrive fællesmængden af disse og det største element i denne vil være den største fællesdivisor. Altså

$$A \cap B = \{1, 2, 3, 4, 6, 12\},$$

hvorfor $\text{sfd}(24, 36) = 12$.

Er der der imod givet de to heltal 10 og 17, ser vi at

$$A = \{1, 2, 5, 10\} \quad \text{og} \quad B = \{1, 17\} \quad \text{og} \quad A \cap B = \{1\},$$

hvorfor $\text{sfd}(10, 17) = 1$. ◇

De heltal hvis største fællesdivisor er 1 er af en så speciel betydning i talteori (hvilket vi senere skal få et indtryk af), at fænomenet har sit eget navn.

Definition 2.8: Indbyrdes primisk
To heltal a og b, hvorom det gælder at de har største fællesdivisor 1, $\text{sfd}(a, b) = 1$*, siges at være* indbyrdes primiske.

Definitionen kan udvides på følgende vis.

Definition 2.9
Heltallene $a_1, a_2, \ldots, a_n$ siges, at være parvis indbyrdes primiske*, hvis den største fællesdivisor af samtlige par af disse heltal er 1. Med symboler skriver vi, hvis* $\text{sfd}(a_i, a_j) = 1$ *når $a \leq i < j \leq n$.*

Eksempel 2.10
Heltallene 10, 17 og 21 er parvis indbyrdes primiske, da

$$\text{sfd}(10, 17) = \text{sfd}(10, 21) = \text{sfd}(17, 21) = 1.$$

Hvis du har brug for at overbevise dig selv kan du ligesom i eksempel 2.7 opskrive mængderne af divisorer og undersøge deres fællesmængder. ◇

2.2 Euklids algoritme og Bézouts identitet

Har man givet to store heltal kan det være næsten umuligt at bestemme største fællesdivisor, eller i bedste fald blot tidskrævende. Heldigvis findes der en metode, eller en algoritme, som løser dette problem for os. Nærmere bestemt er der tale om Euklids algoritme.

For at forstå Euklids algoritme må vi først have et par sætninger på banen. Den første af disse omhandler division, men denne gang den form for division mellem to heltal a og b, hvor disse ikke nødvendigvis går op i hinanden ($b \nmid a$). Hvis $a = 27$ og $b = 6$ ved vi (formentlig) fra skolen, at når 27 deles med 6, så er *kvotienten* 4 og *resten* 3, altså

$$27 = 6 \cdot 4 + 3.$$

Tallet b, her 6, kaldes for *dividenden*. Det er kutyme at opskrive resten r på formen

$$r = a \bmod q,$$

hvor q angiver kvotienten og hvor $a \bmod q$ betyder resten af a ved division med q, en notation som vi skal benytte os flittigt af senere. I eksempelet ovenfor har vi altså

$$27 \bmod 4 = 3.$$

I skolen lærer vi også, at resten skal være mindre end dividenden. At der altid findes netop én sådan rest er præcis essensen af sætning 2.11.

Sætning 2.11
Hvis vi har givet to heltal a og b med $b > 0$, så findes der heltal q og r således, at

$$a = bq + r \quad \text{for} \quad 0 \leq r < b.$$

Heltallet q kaldes her for kvotienten *og heltallet r for* resten*. Der gælder endvidere, at r og q er entydigt fastlagt.*

Bevis *
Vi skal i dette bevis betragte mængden af alle rester $x \geq 0$ til udtrykket $a = by + x$, hvor a, b og y er heltal. Vi kalder denne mængde R og kan skrive den som

$$R = \{x \geq 0 \text{ hvor det gælder, at } a = by + x \text{ for nogle } y \in \mathbb{Z}\}.$$

Det første vi må argumentere for er, at mængden R overhovedet indeholder nogen elementer, altså at den ikke er tom. Hvis $a \geq 0$ viser udtrykket

$$a = b0 + a,$$

at R vil indeholde resten a, mens hvis $a < 0$ viser udtrykket

$$a = a + ba - ba = ba + (1 - b)a,$$

at R indeholder resten $(1 - b)a$. Altså er R ikke tom. Og når R således er en ikke-tom delmængde af de positive hele tal (de naturlige tal med 0) må R også have et mindste element. Vi kalder dette mindste element i R for r. Da $r \in R$ følger det per definitionen af R, at $a = bq + r$ for et eller andet $q \in \mathbb{Z}$. At $r < b$ kan vi vise ved et modstridsbevis. Vi bemærker først, at vi kan foretage følgende omskrivning:

$$a = bq + r = bq + r + b - b = b(q + 1) + (r - b).$$

Dette udtryk indikerer, at hvis $r \geq b$ så ligger $r - b$ i R. Men $r - b$ er jo mindre end r, hvilket er i strid med at r er det mindste element i R. Antagelsen om at $r \geq b$ fører altså til en modstrid og må derfor være falsk. Dette viser, at $r < b$.

Også entydigheden af r og q skal vi vise ved et modstridsbevis. Vi antager, at der findes et heltal q' og et heltal r' således, at

$$a = bq' + r' \quad \text{for} \quad 0 \leq r' < b.$$

Vi opskriver udtrykket

$$r' = a - bq' = a - bq' + bq - bq = (a - bq) + b(q - q')$$

Antag, at $q' < q$. Så vil $q - q' \geq 1$ (da jo q og q' er heltal) og derfor vil $b(q - q') \geq 1$. Da $a - bq = r$ må der gælde, at

$$r' = (a - bq) + b(q - q') \geq r + b \geq b.$$

Men $r' \geq b$ er jo i strid med betingelsen om, at $0 \leq r' < b$, altså er antagelsen $q' < q$ falsk. Det samme argument med q og q' byttet om kan bruges til at vise, at $q < q'$ er falsk. Altså må vi have, at $q = q'$, hvoraf følger at $r = r'$, da

$$r = a - bq = a - bq' = r'.$$

□

Den næste sætning er en såkaldt hjælpesætning, også kaldet et *lemma*, til Euklids algoritme, forstået på den måde at vi senere skal bruge den til at vise korrektheden af algoritmen.

Lemma 2.12
Lad a, b, q og r være heltal sådan at $a = bq + r$. Da gælder, at $\text{sfd}(a, b) = \text{sfd}(b, r)$.

Bevis
Hvis vi kan vise, at mængden af fællesdivisorer af a og b er lig mængden af fællesdivisorer af b og r, så må der nødvendigvis gælde, at $\text{sfd}(a,b) = \text{sfd}(b,r)$, fordi hvis mængderne er de samme så må det største element i de to mængder jo også være det samme.

Antag først, at vi har et heltal d hvorom der gælder, at $d \mid a$ og $d \mid b$. Ifølge sætning 2.3 (*ii*) findes der da et heltal q således, at $d \mid bq$ og der vil også gælde at $d \mid -bq$. Ifølge sætning 2.3 (*i*) har vi, da $d \mid a$ (per antagelse) og $d \mid -bq$, at $d \mid a - bq$. Da $r = a - bq$ har vi altså, at $d \mid r$. Altså vil enhver fællesdivisor af a og b også være en fællesdivisor af b og r.

Dernæst antages, at et heltal d er divisor i både b og r, altså at $d \mid b$ og $d \mid r$. På tilsvarende vis som ovenfor kan vi her udlede, at $d \mid bq + r = a$, altså at enhver fællesdivisor af b og r også er en fællesdivisor af a og b.

Mængden af fællesdivisorer for a og b henholdsvis b og r er altså ens, hvorfor de to par af heltal også må have samme største fællesdivisor. □

Eksempel 2.13
Hvis vi har $36 = 24 \cdot 1 + 12$ svarende til $a = bq + r$ vil $\text{sfd}(36,24) = \text{sfd}(24,12)$. Vi ved fra tidligere, at $\text{sfd}(36,24) = 12$ og at $\text{sfd}(24,12)$ også er lig 12 er let at overbevise sig om. ◇

Nu er vi klar til at formulere Euklids algoritme.

Algoritme 2.14: Euklids algoritme
Lad inddata i algoritmen være to heltal a og b med $b > 0$ og $a \geq b$. Første skridt er at sætte $a = r_0$ og $b = r_1$. De følgende skridt består i at anvende sætning 2.11 gentagende gange, hvorved fås:

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 \\
r_1 &= r_2 q_2 + r_3 \\
&\vdots \\
r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1} \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n \\
r_{n-1} &= r_n q_n,
\end{aligned}$$

hvor $r_0 > r_1 > r_2 > \ldots \geq 0$. Uddata for algoritmen er den sidste rest r_n forskellig fra 0 i følgen af rester r_i for $i = 1, 2, \ldots, n$. Denne rest er lig $\text{sfd}(a,b)$.

Fra afsnit 1.4 ved vi at en algoritme bør opfylde syv krav. Opfyldelsen af de fleste af disse krav følger forholdsvist nemt af formuleringen af algoritmen ovenfor, men to af dem kræver lidt mere argumentation.

Sætning 2.15
Der gælder, at Euklids algoritme opfylder kravene om terminering og korrekthed, hvor der med korrekthed forstås, at $\text{sfd}(a,b) = r_n$.

Bevis
Det første vi bemærker er, at følgen af rester

$$a = r_0 > b = r_1 > r_2 > \ldots > r_{n-1} > r_n \geq 0$$

maksimalt kan indeholde a led, hvorfor den vil terminere samt at et nul derfor vil optræde til sidst. Dette betyder at også algoritmen vil komme til et naturligt stop.

Korrektheden følger af lemma 2.12, da vi ifølge dette har, at

$$\text{sfd}(a,b) = \text{sfd}(r_0, r_1) = \text{sfd}(r_1, r_2) = \ldots = \text{sfd}(r_{n-1}, r_n) = \text{sfd}(r_n, 0) = r_n.$$

Altså er $\text{sfd}(a,b) = r_n$, den sidste rest forskellig fra 0 i følgen af rester ved gentagende division. □

Et par eksempler på hvordan vi så rent faktisk udfører Euklids algoritme er nok på sin plads nu.

Eksempel 2.16
Vi begynder med et simpelt eksempel, nemlig at anvende Euklids algoritme til at bestemme $\text{sfd}(24, 36)$:

$$\begin{aligned} 36 &= 24 \cdot 1 + 12 \\ 24 &= 12 \cdot 2 + 0 \end{aligned}$$

Heraf følger, at $\text{sfd}(24, 36) = 12$, som vi har argumenteret for ved flere tidligere lejligheder. Men lad os se algoritmen udført på nogle andre og lidt større tal, lad os bestemme $\text{sfd}(414, 662)$:

$$\begin{aligned} 662 &= 414 \cdot 1 + 248 \\ 414 &= 248 \cdot 1 + 166 \\ 248 &= 166 \cdot 1 + 82 \\ 166 &= 82 \cdot 2 + 2 \\ 82 &= 2 \cdot 41 + 0 \end{aligned}$$

Det følger heraf, at $\text{sfd}(414, 662) = 2$. ◇

På baggrund af Euklids algoritme kan man opskive en lille og nyttig sætning, kaldet Bézouts identitet efter den franske matematiker Étienne Bézout (1730-1783).

Sætning 2.17: Bezouts identitet
Lad a og b være heltal med $b \geq 0$, da findes der heltal s og t, således at

$$\text{sfd}(a,b) = sa + tb.$$

Bevis
Fra sætning 2.15 ved vi at $\text{sfd}(a,b) = r_n$. Fra samme sætning ved vi ligeledes, at

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \quad \Leftrightarrow \quad r_n = r_{n-2} - r_{n-1}q_{n-1}.$$

Det betyder, at vi kan opskrive $\text{sfd}(a,b)$ på formen

$$\text{sfd}(a,b) = s'r_{n-1} + t'r_{n-2},$$

hvor $s' = -q_{n-1}$ og $t' = 1$. Vi kan dernæst udtrykke r_{n-1} i termer af r_{n-2} og r_{n-3}. Fra Euklids algoritme (algoritme 2.14) har vi, at

$$r_{n-3} = r_{n-2}q_{n-2} + r_{n-1} \quad \Leftrightarrow \quad r_{n-1} = r_{n-3} - r_{n-2}q_{n-2}.$$

Vi får da, at

$$\text{sfd}(a,b) = s'(r_{n-3} - r_{n-2}q_{n-2}) + t'r_{n-2},$$

hvilket kan skrives på formen

$$\text{sfd}(a,b) = s''r_{n-2} + t''r_{n-3},$$

hvor $s'' = t' - s'q_{n-2}$ og $t'' = s'$. Fortsætter vi på denne måde vil vi til sidst opnå et udtryk på den ønskede form, $\text{sfd}(a,b) = sa + tb$, med udtryk for værdierne af s og t. □

Eksempel 2.18
I det tilfælde hvor vi med Euklids algoritme ovenfor beregnede $\text{sfd}(414, 662) = 2$ kan vi opskrive følgende:

$$\begin{aligned} 2 &= 166 - 82 \cdot 2 = 1 \cdot 166 + (-2) \cdot 82 \\ &= 1 \cdot 166 + (-2) \cdot (248 - 166 \cdot 1) = (-2) \cdot 248 + 3 \cdot 166 \\ &= (-2) \cdot 248 + 3 \cdot (414 - 248 \cdot 1) = 3 \cdot 414 + (-5) \cdot 248 \\ &= 3 \cdot 414 + (-5) \cdot (662 - 414 \cdot 1) = (-5) \cdot 662 + 8 \cdot 414. \end{aligned}$$

Altså kan vi ved at indsætte 'baglæns' i Euklids algoritme bestemme de to heltal s og t til henholdsvis -5 og 8 således, at $\text{sfd}(414, 662)$ kan udtrykkes som en sum af netop 414 og 662:

$$\text{sfd}(414, 662) = (-5) \cdot 662 + 8 \cdot 414.$$

◇

I det tilfælde hvor a og b er indbyrdes primiske, altså $\text{sfd}(a,b) = 1$, har vi $1 = sa + tb$. Og det er netop dette specialtilfælde af Bézouts identitet som vi skal bruge i næste afsnit. Med udgangspunkt i Bézouts identitet kan vi også vise følgende mindre sætning, som vi senere skal bruge i kapitel 3.

Sætning 2.19
Lad a, b og c være positive heltal således, at a og b er indbyrdes primiske og lad endvidere $a \mid bc$. Da gælder, at $a \mid c$.

Bevis
Da $\text{sfd}(a, b) = 1$ findes der ifølge Bézouts identitet heltal s og t, således at $sa + tb = 1$. Ved at gange igennem med c får vi, at $csa + ctb = c$. Af sætning 2.3 (*ii*) følger, at $a \mid ctb$, da vi jo som forudsætning har at $a \mid bc$. Da vi således har, at $a \mid csa$ og $a \mid ctb$ følger af sætning 2.3 (*i*), at $a \mid csa + ctb$, altså at $a \mid c$. □

2.3 Primtal og aritmetikkens fundamentalsætning

Som sagt har nogle af heltallene en hel speciel egenskab – en egenskab der har gjort dem til genstand for studier igennem årtusinder – nemlig at det for et sådant heltal kun er tallet selv og 1 der går op i tallet. Disse heltal kaldes for *primtal*. En mere formel definition af primtal er den følgende.

Definition 2.20: Primtal
Et heltal $p > 1$ kaldes et primtal*, hvis de eneste positive faktorer i p er 1 og p selv.*

Strengt taget kunne man godt have medregnet tallet 1 som værende et primtal, men det viser sig at mange ting bliver lettere, hvis man ikke gør det. Det første, og eneste lige primtal (hvorfor?), er således tallet 2.

Eksempel 2.21
Primtallene op til 100 er:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$

$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

◇

Heltal der ikke er primtal er *sammensatte tal*, disse kan vi også definere formelt.

Definition 2.22: Sammensat tal
Et heltal n kaldes et sammensat tal*, hvis og kun hvis der eksisterer et heltal a således, at $a \mid n$ og $1 < a < n$.*

Eksempel 2.23
Heltallet $6 = 2 \cdot 3$, hvor såvel 2 som 3 opfylder kriteriet for a i definition 2.22. Altså er 6 et sammensat tal. ◇

I og med at både 2 og 3 er primtal siges disse også at være *primdivisorer* i det sammensatte tal 6. Når man på denne måde splitter et heltal op i et produkt af primtal siger man også, at man har *primfaktoriseret* heltallet. Grunden til at der er tale om primfaktoriserin*gen* og ikke blot *en* primfaktorisering er, at denne for et givet heltal er *entydig* (på nær

ombytning af primdivisorerne). Hvis 6 således skal udtrykkes som et produkt af primtal kan det altså kun udtrykkes som $2 \cdot 3$ (eller $3 \cdot 2$). Dette resultat er en del af *aritmetikkens fundamentalsætning*. Men for at vise den skal vi bruge et lemma.

For at bevise dette lemma skal vi imidlertid have fat i en speciel form for bevisteknik kaldet bevis ved induktion eller *induktionsprincippet*. Vi kender allerede to former for bevisteknikker, den direkte og den indirekte (bevis ved modstrid), og induktionsprincippet er altså en tredje. Bevis ved induktion bruges ofte til at vise at en given sætning er sand for alle naturlige tal. Det første kendte eksempel på bevis ved matematisk induktion findes i den italienske matematiker Francisco Maurolicos (1494-1575) *Arithmeticorum libri duo* fra 1575. Maurolico brugte induktion til at vise, at der altid gælder at summen af de første n ulige naturlige tal er n^2. Hvis man kigger på de første eksempler er det jo rimeligt at antage, at det forholder sig sådan:

$$\begin{aligned} 1 &= 1^2 \\ 1+3 &= 2^2 \\ 1+3+5 &= 3^2 \\ 1+3+5+7 &= 4^2 \\ 1+3+5+7+9 &= 5^2 \\ 1+3+5+7+9+11 &= 6^2 \\ &\vdots \end{aligned}$$

Men en anden ting er selvfølgelig at vise det helt generelt. Ideen er, at hvis det gælder for $n = 1$, hvilket det som set ovenfor gør da $1 = 1^2$, så antager man at det gælder for $n = k$ og kan man så vise det også gælder for $n = k + 1$, så må det gælde for alle n. Dette er *induktionsprincippet*. Tilfældet $n = 1$ kaldes for *induktionsbasis* og antagelsen $n = k$ kaldes for *induktionshypotesen*. Det er vigtigt, at pointere at selve induktionsprincippet ikke er noget man kan eftervise, deraf navnet princip. I virkeligheden kan man tænke på det som en form for axiom, som indgår i grundlaget for de naturlige tal.

Et billede som man kan have af induktionsprincippet inde i sit hoved, er det af uendeligt mange dominobrikker opstillet på en lang række. Hvis den første dominobrik, $n = 1$, vælter, så vil også den næste, $n = 2$, vælte. Hvis dominobrik $n = 2$ vælter, så vil også dominobrik $n = 3$ vælte. Og hvis $n = 3$ vælter, så vil også $n = 4$ vælte og så kører maskinen. Denne 'dominoeffekt' kan vi også tænke på '*induktionsmotoren*'. Vores induktionsbasis vil her være at den første dominobrik vælter, $n = 1$, hvilket vi vil kunne stadfæste ved rent faktisk at vælte den. Induktionshypotesen er at den k'te dominobrik også vælter, $n = k$. Hvis vi kan godtgøre, at dominobrik nummer $k + 1$ ligeledes vælter, så siger induktionsprincippet, at alle brikkerne vælter.

Men lad os nu se om vi kan vise Maurolico's sætning ved hjælp af induktionsprincippet.

Eksempel 2.24 (Induktionsbevis for Maurolicos sætning)
Sætning: Summen af de første n ulige positive heltal er n^2.

Vores induktionsbasis er som sagt $n = 1$, altså at sætningen holder i det første tilfælde, hvilket den gør da $1 = 1^2$.

Induktionshypotesen er at sætningen også holder i tilfældet $n = k$, hvilket vi kan opskrive som

$$1 + 3 + \ldots + (2k - 1) = k^2,$$

da det k'te positive ulige heltal er givet ved $2k - 1$, idet det jo bestemmes ved at lægge 2 til 1 $k - 1$ gange: $2(k - 1) + 1 = 2k - 1$.

Vi skal så vise resultatet for $n = k+1$, hvilket, da $2(k+1)-1 = 2k+1$, vil sige

$$1 + 3 + \ldots + (2k - 1) + (2k + 1) = (k + 1)^2,$$

eller vi kan forklare det ved, at det $k+1$'te positive ulige heltal bestemmes ved at lægge 2 til 1 k gange, altså $2k + 1$. Ideen med induktionshypotesen er, at det er en antagelse og man har således lov til at bruge den til at vise tilfældet $n = k + 1$. Vi kan derfor opskrive følgende:

$$\begin{aligned} 1 + 3 + \ldots + (2k - 1) + (2k + 1) &= [1 + 3 + \ldots + (2k - 1)] + (2k + 1) \\ &= k^2 + (2k + 1) \\ &= k^2 + 2k + 1 \\ &= (k + 1)^2. \end{aligned}$$

Dette viser, at tilfældet $n = k + 1$ følger fra induktionshypotesen (som blev anvendt ovenfor til at omskrive udtrykket). Da vores induktionsbasis er sand og tilfældet $n = k + 1$ følger fra induktionshypotesen for alle positive heltal k er sætningen ifølge induktionsprincippet sand for alle positive heltal n. ◇

Og nu skulle vi så være klar til at bevise vores lemma ved brug af induktionsprincippet.

Lemma 2.25
Hvis p er et primtal og $m_1, m_2, \ldots, m_n$ er heltal således at

$$p \mid m_1 m_2 \cdots m_n,$$

så gælder der, at $p \mid m_i$ for (mindst) et m_i med $1 \leq i \leq n$.

Bevis
For vores induktionsbasis ser vi altså på $n = 1$. Det er åbenlyst, at sætningen gælder i dette tilfælde, da produktet jo kun består af heltallet m_1. Som vores induktionshypotese antager vi, at sætningen også gælder for $n = k$. Kan vi nu vise, at den ligeledes gælder for $n = k + 1$ er vi i hus.

Vi antager altså, som sætningen forudsætter, at $p \mid m_1 m_2 \cdots m_k m_{k+1}$ og sætter derefter $m = m_1 m_2 \ldots m_k$. Vi skal så vise, at p går op i et af

m_i'erne for $i = 1, \ldots, k+1$. Vi kan gøre dette ved at betragte følgende to tilfælde: (1) $p \mid m$ og (2) $p \nmid m$.

(1) Hvis $p \mid m$ har vi ifølge induktionshypotesen, at $p \mid m_i$ for et m_i med med $1 \leq i \leq n$, og dermed gælder sætningen.

(2) Hvis derimod $p \nmid m$ har vi, da p jo er et primtal og derfor ikke har andre divisorer end 1 og sig selv, at $\text{sfd}(p, m) = 1$. Fra specialtilfældet af sætning 2.17 (Bezouts identitet) ved vi, at der findes heltal s og t, således at $sp + tm = 1$. Vi kan derfor opskrive følgende udtryk

$$m_{k+1} = 1 \cdot m_{k+1} = (sp + tm)m_{k+1} = (sm_{k+1})p + t(mm_{k+1}).$$

Da p går op i begge udtryk på højre side af det sidste lighedstegn, $p \mid p$ og som forudsat ovenfor haves at $p \mid mm_{k+1}$, har vi ifølge sætning 2.3 (i), at $p \mid m_{k+1}$.

I begge tilfælde går p altså op i et af m_i'erne for $1 \leq i \leq k+1$ og ifølge induktionsprincippet er resultatet altså sandt for alle positive heltal n. □

En til tider forekommende fejl er at lemma 2.25 forbliver sand, når primtallet p udskiftes med et vilkårligt heltal. Men dette er åbenlyst ikke sandt, for eksempel har vi, at $6 \mid 3 \cdot 4$, men $6 \nmid 3$ og $6 \nmid 4$. Der er altså i lemma 2.25 tale om en helt speciel egenskab ved netop primtal.

Ved hjælp af lemma 2.25 er vi nu i stand til at vise vores hovedresultat, aritmetikkens fundamentalsætning, som siger at ethvert heltal større end 1 kan opskrives entydigt som (1) enten et primtal eller (2) et produkt af to eller flere primtal (ordnet efter størrelse).

Sætning 2.26: Aritmetikkens fundamentalsætning
Ethvert heltal m større end 1 kan skrives som et produkt af primtal. Der gælder endvidere at dette produkt er entydigt bestemt, bortset fra rækkefølgen af primtallene.

Beviset for aritmetikkens fundamentalsætning er heunder delt op i beviset for eksistensen og beviset for entydigheden.

Bevis
Vi begynder med eksistensen, altså at ethvert heltal større end 1 har en primfaktorisering, eller med andre ord at det kan skrives som et produkt af primtal. Beviset føres ved modstrid, hvorfor vi begynder med at antage, at der findes heltal som ikke kan skrives som et produkt af primtal. Der må da være et mindste af disse, dette kalder vi m. Heltallet m kan ikke selv være et primtal, idet ethvert primtal jo i sig selv er et produkt af primtal. Altså må m være et sammensat tal. Det vil sige $m = ab$, hvor både a og b er heltal mindre end m. Da m jo per antagelse er det mindste heltal som ikke kan skrives som produkt af primtal må både a og b nødvendigvis kunne skrives som produkter af primtal. Men så kan $m = ab$ jo også skrives som et produkt af primtal. Altså har vi en modstrid og antagelsen om at der findes heltal som ikke kan skrives som et produkt af primtal må forkastes. □

Bevis *
Beviset for entydigheden føres ligeledes ved modstrid. Antag, at der findes heltal som ikke har en entydig primfaktorisering, altså at de kan skrives som produkter af primtal på flere forskellige måder. Der må da findes et mindste sådant heltal, lad os kalde det m, med to forskellige primfaktoriseringer

$$p_1 p_2 p_3 \cdots p_k = q_1 q_2 q_3 \cdots q_l = m,$$

hvor p_i er primtal med $1 \leq i \leq k$, ikke nødvendigvis forskellige, og q_j er primtal med $1 \leq j \leq l$, ligeledes ikke nødvendigvis forskellige. Af første ligning ses, at $p_1 \mid m$, hvoraf vi kan drage den konklusion, at primtallet p_1 ligeledes må gå op i m's anden primfaktorisering, altså $p_1 \mid m = q_1 q_2 q_3 \cdots q_l$. Af lemma 2.25 følger det, at $p_1 \mid q_j$ for et eller andet j $(1 \leq j \leq l)$. Ved at bytte om på rækkefølgen af primtallene i m's anden primfaktorisering kan vi opnå, at $p_1 \mid q_1$, og da både p_1 og q_1 er primtal må der nødvendigvis gælde, at $p_1 = q_1$. Vi kan da faktorisere disse to primtal ud af m's primfaktoriseringer

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_l = n.$$

Primfaktoriseringerne af m var jo per antagelse forskellige, og efter som de to primtal vi har fjernet var ens, må n jo også have to forskellige primfaktoriseringer. Men $n < m$ hvilket strider imod vores definition af m som det mindste heltal uden entydig primfaktorisering. Altså har vi en modstrid, hvorfor vores antagelse om at der findes heltal større end 1 uden entydige primfaktoriseringer må forkastes. □

Vi har allerede set at heltallet 6 har primfaktoriseringen $2 \cdot 3$, men lad os se et par eksempler mere.

Eksempel 2.27
Heltallet $256 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^8$. Heltallet 990 kan skrives som $990 = 2 \cdot 3^2 \cdot 5 \cdot 11$. Heltallet 1117 er et primtal og kan derfor kun skrives som 1117. ◇

Beviset for aritmetikkens fundamentalsætning er *ikke-konstruktivt*, hvormed forstås at det kun siger at der eksisterer en primfaktorisering for alle heltal og at denne primfaktorisering er entydig, beviset giver ikke nogen konstruktiv metode til, hvordan man bestemmer denne primfaktorisering. Det at bestemme primfaktoriseringen af et meget stort heltal, eksempelvis et på flere tusinde cifre, er selv med den i dag hurtigste computer en ekstremt tidskrævende proces – der kendes i alt fald på nuværende tidspunkt ingen metode der kan gøre det inden for en overskuelig tidshorisont. Og som vi skal se i kapitel 4 er det netop dette som kryptering med primtal bygger på.

En ting er at kende primfaktoriseringen af givne heltal en anden, omend beslægtet, ting er at bestemme om et givet heltal er et primtal eller et sammensat tal. For små heltal, som tallet 6, er dette nemt at overskue, men hvad gør man når man skal bestemme om store heltal er

primtal eller sammensatte tal? Den første og mest åbenlyse test går på om tallet er lige eller ulige. Det eneste lige primtal er som set tallet 2, alle andre lige tal er sammensatte tal, idet 2 jo er en primdivisor i disse. Ifølge aritmetikkens fundamentalsætning ved vi, at ethvert heltal kan skrives som et produkt af primtal, så den næste åbenlyse test er da for et givet heltal n at dividere samtlige primtal $p < n$ op i n. Går et af dem op i n er n et sammensat tal, gør ingen af dem er n et primtal.

Eksempel 2.28
Er heltallet 101 et primtal? Ifølge testen ovenfor skal vi for at finde ud af dette dividere primtallene op til 100 (jævnfør eksempel 2.21) op i 101. Hvad bliver konklusionen? ◇

Testen i ovenstående eksempel er noget omstændelig og faktisk heller ikke helt gennemtænkt, idet vi jo for eksempel kan sige os selv, at 97 ikke går op i 101. Det gør $98, 83, \ldots, 53$ åbenlyst heller ikke. Så vi behøver altså ikke prøve med alle $p < n$. Spørgsmålet er så, hvor mange, eller hvor få, vi kan nøjes med for at undersøge om et heltal er et primtal. Heldigvis har vi en sætning der fortæller os dette.

Sætning 2.29
Hvis n er et sammensat tal, så har n en primdivisor som er mindre end eller lig $\sqrt{n}$.

Bevis *
Hvis n er et sammensat tal er $n = ab$ for et a og et b større end 1. Bemærk, at vi enten har, at $a \leq \sqrt{n}$ eller at $b \leq \sqrt{n}$, da vi jo i modsat fald ville have, at $ab > \sqrt{n} \cdot \sqrt{n} = n$, hvilket er i strid med definitionen af et sammensat tal. Altså, har n en positiv divisor som ikke overstiger $\sqrt{n}$. Ifølge aritmetikkens fundamentalsætning er denne divisor enten et primtal eller har selv en primdivisor. I hvert tilfælde har n en primdivisor som er mindre end eller lig $\sqrt{n}$. □

I termer af primtal kan sætning 2.29 også omformuleres til følgende korollar.

Korollar 2.30
Et heltal er et primtal, hvis det ikke er deleligt med noget primtal mindre end eller lig dets kvadratrod.

Lad os atter se på vores eksempel fra før.

Eksempel 2.31
Vi ser igen på heltallet 101. Da $\sqrt{101} = 10,0499$ skal vi ifølge ovenstående korollar kun se på primtal $p \leq 10$, det vil sige 2,3,5 og 7. Da ingen af disse går op i 101 er 101 altså et primtal. ◇

Som nævnt indeholder Elementerne en sætning kendt som Euklids sætning. Der er tale om en særdeles berømt sætning (og et mindst lige så berømt bevis!) inden for matematikken, og derfor også talteorien, som udtaler sig om intet mindre end hvor mange primtal der findes.

Sætning 2.32: Euklids sætning
Der er uendeligt mange primtal.

Bevis
Beviset føres ved modstrid. Antag, at der kun er en endelig mængde primtal $\{p_1, p_2, \ldots, p_n\}$ og lad heltallet q være givet ved

$$q = p_1 p_2 \cdots p_n + 1.$$

Ifølge aritmetikkens fundamentalsætning er q enten selv et primtal eller er et produkt af primtal. Men ingen af primtallene $p_1, p_2, \ldots, p_n$ går op i q. De går op i $p_1 p_2 \cdots p_n$, men for at de også skal gå op i q skal de gå op i differensen mellem $p_1 p_2 \cdots p_n$ og q, hvilket er 1. Ifølge aritmetikkens fundamentalsætning må q altså selv være et primtal, hvilket fører til en modstrid med vores oprindelige antagelse. Ergo må der findes uendeligt mange primtal. □

Lad os se et eksempel på det som Euklid benytter sig af i sit bevis.

Eksempel 2.33
Hvis vi forestiller os, at vi kun kender de tre første primtal, så kan vi opskrive den endelige mængde bestående af disse, altså $\{2, 3, 5\}$. Vi kan derefter beregne q til

$$q = 2 \cdot 3 \cdot 5 + 1 = 31.$$

31 skulle så være et primtal, og det er det også. Hvis man skulle være i tvivl kan man selvfølgelig vise det ved at udregne $\sqrt{31} = 5,56776$ og derefter dividere primtallene mindre end eller lig 5 op i 31. Disse er jo netop 2, 3 og 5, som vi grundet konstruktionen af q ved ikke går op i 31. Altså har vi ved hjælp af alle de primtal vi kendte beregnet et nyt og større primtal. ◇

Det faktum at der findes uendeligt mange primtal gør det selvfølgelig muligt hele tiden at finde større og større primtal. Og faktisk har det at have rekorden for at have fundet det pt. største kendte primtal udviklet sig til lidt af en 'sport' blandt talentusiaster.

2.4 Jagten på større og større primtal

Der findes ingen generel formel til at beregne det næste primtal i følgen af primtal. Faktisk er et af de helt store spørgsmål i matematikken, hvordan primtallene præcist fordeler sig jo længere og længere man bevæger sig ud af den positive tallinie – man ved noget, men slet ikke alt. (Vi skal studere dette lidt nærmere i slutningen af kapitel 3.) Der findes dog en hel del måder til at konstruere primtal, eller oftere med en vis sandsynlighed at konstruere primtal. Eksempelvis kan man vise, at der findes uendeligt mange primtal af formen $(4n + 3)$, hvor n er et positivt heltal. For $n = 0, 1, 2, \ldots$ får vi følgen af primtal på denne form til

$$3, 7, 11, 19, 23, 31, 43, 47, \ldots$$

(bemærk, at $n = 3, 6, 8, 9$ ikke giver anledning til primtal). Ligeledes gælder det, at der findes uendeligt mange primtal af typen $(4n + 1)$, og faktisk er alle primtal fra 5 og frem enten af typen $(4n + 1)$ eller af typen $(4n + 3)$. Et interessant spørgsmål er imidlertid om der findes flest primtal af typen $(4n + 1)$ eller af typen $(4n + 3)$ efterhånden som man arbejder sig ud af tallinien – dette er kendt som *primtalskapløbet*. Hvis man begynder at tælle kunne man få den opfattelse, at det altid vil være $(4n + 3)$ der fører dette kapløb (jævnfør følgen ovenfor af primtal på formen $(4n + 3)$), men faktisk viser det sig at $(4n + 1)$ overtager føringen ved 26861, som er et primtal af type $(4n + 1)$. På dette tidspunkt er der 1473 primtal af typen $(4n + 1)$, mens der kun er 1472 primtal af typen $(4n + 3)$. De to typer fortsætter med at skifte føring på en højst irregulær vis jo længere man bevæger sig ud af tallinien. For hovedparten af de første få milliarder fører $(4n + 3)$, men hvad der sker jo længere vi bevæger os ud af tallinien er uvist. Det sjette og største kendte område, hvor $(4n + 1)$ fører ligger mellem 18.465.126.293 og 19.033.524.538. Et lignende kapløb finder sted mellem de to slags primtal af henholdsvis formen $3n + 2$ og $3n + 1$.

Så ét spørgsmål går altså på primtallenes fordeling på tallinien, ét andet spørgsmål går imidlertid på at finde store primtal. Dette spørgsmål har interesseret matematikere i flere århundreder, men med anvendelsen af talteori i kryptering er spørgsmålet kun blevet mere relevant. For at RSA-kryptering fungerer er man, hvilket vil blive forklaret i detaljer i kapitel 4, nødt til at kende to store primtal p og q. Og 100-200 cifre i hver af disse primtal er langt fra unormalt. Men hvordan finder man sådanne store primtal? Dette problem diskuterede allerede den franske munk, filosof og matematiker Marin Mersenne (1588-1648) i sin bog *Cogitata Physico-Mathematica* fra 1644. Mersennes ide var at kigge på naturlige tal af typen $2^n - 1$ for $n = 1, 2, 3, \ldots$, de i dag såkaldte *Mersenne-tal*, M_n. Der gælder følgende sætning om disse tal.

Sætning 2.34
Hvis $2^n - 1$ er et primtal, så er n et primtal.

Bevis *
Antag, at n ikke er et primtal, hvilket vil sige at det har en primfaktor p. I så fald vil $2^p - 1$ gå op i $2^n - 1$, idet $n = pq$ giver, at

$$2^n - 1 = (2^p - 1)(2^{pq-p} + \ldots + 2^p + 1).$$

Men dette giver anledning til en modstrid, da $2^n - 1$ derfor ikke som forudsat er et primtal. Altså må n nødvendigvis være et primtal. □

Det modsatte gælder imidlertid ikke altid: Hvis n er et primtal, så er $M_n = 2^n - 1$ måske et primtal, men ikke nødvendigvis. Mersenne fremførte i sin bog fra 1644 den påstand, at for alle $n = 1, \ldots, 257$ er $M_n = 2^n - 1$ kun primtal for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$. Noget af det mest bemærkelsesværdige i denne sammenhæng er, at Mersenne var i stand til at jonglere med så store tal, tallet M_{127} er for eksempel et tal på 39 cifre:

$$M_{127} = 170141183460469231731687303715884105727.$$

Og hvordan kunne han være sikker på at der rent faktisk var tale om primtal? På Mersennes tid fandtes der ikke pålidelige metoder til at teste om et givet heltal er primtal eller ej. Faktisk forekommer der da også mangler såvel som fejl i Mersennes liste. I 1883 blev det vist, at M_{61} er et primtal som mangler på Mersennes liste. I 1903 blev det vist, at tallet M_{67} på Mersennes liste faktisk er sammensat. I henholdsvis 1911 og 1914 blev det vist, at M_{89} og M_{107} ligeledes er primtal som mangler på Mersennes liste. Først efter anden verdenskrig blev Mersennes liste endegyldigt afprøvet og det blev fundet at M_{257} også er et sammensat tal. Den korrekte liste af *Mersenne-primtal* op til og med $n = 257$ består altså af $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$.

Selv om Mersenne havde fremsat sin liste af Mersenne-primtal var der stadig kun tale om en påstand, idet han ikke havde godtgjort at der rent faktisk var tale om primtal. Matematikeren Leonhard Euler (1707-1783) viste imidlertid i 1750, at M_{31} rent faktisk er et primtal. M_{31} forblev det største kendte primtal frem til 1876, hvor en anden matematiker Édouard Lucas (1842-1891) viste, at M_{127} ligeledes er et primtal. M_{127} holdt rekorden som det største kendte primtal helt frem til begyndelsen af 1950'erne og det er stadig det største primtal der nogensinde er blevet beregnet med håndkraft. Fra 1952 og frem har opdagelsen af nye Mersenne-primtal imidlertid taget fart, hvilket selvfølgelig skyldes brugen af computere til beregning og tests af sådanne. I 1952 blev de næste fem Mersenne-primtal i rækken, nr. 13, 14, 15, 16, og 17, således fundet. Disse er tallene M_{521}, M_{607}, M_{1279}, M_{2203} og M_{2281} med følgende antal af cifre 157, 183, 386, 664 og 687. Fundet skyldtes den amerikanske matematiker Raphael M. Robinson (1911-1995). Rekorden for det størst kendte primtal blev i 1978 holdt af to 18-årige studerende ved California State University, Laura Nickel og Curt Noll, som begge siden gymnasietiden havde interesseret sig for computerberegninger. De fandt det 25. Mersenne-primtal, M_{21701}, et tal med 6.533 cifre, ved at køre deres program på den centrale CYBER 174 computer i Los Angeles. Noll fandt året efter det 26. Mersenne-primtal, M_{23209}. Oftest forholder det sig sådan, at det størst kendte primtal er et Mersenne-primtal, men der er få undtagelser. Et eksempel på dette er primtallet $391581 \cdot 2^{216193} - 1$ på 65.087 cifre som holdt rekorden fra 1989 til 1992. Fundet skyldtes gruppen Amdahl Six, som Noll også er medlem af, og blev gjort på en Amdahl 1200 maskine. Det i dag størst kendte primtal er atter et Mersenne-primtal, nærmere bestemt $M_{32582657}$ som er på 9.808.358 cifre og blev fundet af Cooper og Boone i 2006 på en Pentium 4 (3 GHz) som del af GIMPS-projektet.

GIMPS (Great Internet Mersenne Prime Search) blev begyndt af datalogen George Woltman og er et eksempel på distribuerede beregninger. Ideen i distribuerede beregninger er, at de tilsluttede hjemmepc'er løbende bliver tildelt beregningsopgaver via Internettet. Disse opgaver kører så hele tiden i baggrunden på computeren på en sådan vis at maskinen konstant udnytter den ledige processorkraft. I begyndelsen af 1996 lagde Woltman alle kendte resultater om Mersenne-primtal ud på nettet sammen med et hurtigt program til at teste om et Mersenne-tal er et primtal. Snart deltog tusindvis af eksperter såvel som amatører i projektet og allerede senere samme år begyndte de første resultater at dukke op. Og rekorden for størst kendte primtal har siden

1996 været holdt af deltagere i GIMPS-projektet. GIMPS-projektet vil sikkert fortsætte mange år fremover, for som vi ved findes der jo uendeligt mange primtal og ifølge matematikeren Guy (1994) findes der formodentlig også uendeligt mange Mersenne-primtal, selv om der ikke findes et bevis herfor.

2.5 Opgaver

Opgave 12
Forklar hvad der forstås ved følgende begreber: Naturlige tal, heltal, 'at gå op i', største fællesdivisor, indbyrdes primisk, primtal, sammensat tal, primtalskapløbet, Mersenne-tal, Mersenne-primtal, GIMPS, distribuerede beregninger.

Opgave 13
Forklar hvad der forstås ved et direkte bevis, et inddirekte bevis (også kaldet et modstridsbevis) og et induktionsbevis.

Opgave 14
Hvad siger aritmetikkens fundamentalsætning? Og hvorfor er den fundamental?

Opgave 15
Vis ved hjælp af definition 2.1, at hvis $a \neq 0$ er et heltal, så vil for det første $1 \mid a$ og for det andet $a \mid 0$.

Opgave 16
Vis følgende:

a. Hvis a og b er heltal således at $a \mid b$ og $b \mid a$, så er enten $a = b$ eller $a = -b$.
b. Hvis a, b, c og d er heltal således at $a \mid c$ og $b \mid d$, så vil $ab \mid cd$.
c. Hvis a, b og c er heltal således, at $ac \mid bc$, så vil $a \mid b$.

Opgave 17
Hvad er største fællesdivisor af følgende par af heltal?

a. $3^7 \cdot 5^3 \cdot 7^3$ og $2^{11} \cdot 3^5 \cdot 5^9$.
b. $11 \cdot 13 \cdot 17$ og $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$.
c. 23^{31} og 23^{17}.
d. $41 \cdot 43 \cdot 53$ og $41 \cdot 43 \cdot 53$.
e. 1013 og 0.

Opgave 18
Hvilke positive heltal findes der som er:

a. Mindre end 12 og indbyrdes primiske med 12?
b. Mindre end 30 og indbyrdes primiske med 30?

Opgave 19
Undersøg om heltallene i de følgende mængder er parvis indbyrdes primiske.
a. 11, 15, 19.
b. 12, 17, 31, 37.
c. 14, 15, 21.
d. 7, 8, 9, 11.

Opgave 20
Udover at tale om største fællesdivisor kan man også tale om *mindste fællesmultiplum*, hvilket er formuleret således:

Definition 2.35: Mindste fællesmultiplum
Lad a og b være heltal større end nul. Det mindste fælles multiplum *af a og b, skrevet* $\mathrm{mfm}(a, b)$*, er det mindste heltal deleligt med både a og b.*

Bestem mindste fællesmultiplum af følgende par af heltal:
a. $3^7 \cdot 5^3 \cdot 7^3$ og $2^{11} \cdot 3^5 \cdot 5^9$.
b. $11 \cdot 13 \cdot 17$ og $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$.
c. 23^{31} og 23^{17}.
d. $41 \cdot 43 \cdot 53$ og $41 \cdot 43 \cdot 53$.
e. 1013 og 0.

Opgave 21
Hvad er kvotienten q og resten r, når:
a. 19 divideres med 7?
b. -111 divideres med 11?
c. 1001 divideres med 13?
d. 0 divideres med 19?
e. 3 divideres med 5?

Opgave 22
Udregn følgende udtryk:
a. $13 \bmod 3$.
b. $155 \bmod 19$.
c. $-101 \bmod 13$.
d. $199 \bmod 19$.
e. $-97 \bmod 11$.
f. $-221 \bmod 23$.
g. $777 \bmod 7$.

Opgave 23
Argumenter for at Euklids algoritme opfylder de resterende fem krav, det vil sige dem udover terminering og korrekthed, for algoritmer angivet i afsnit 1.4.

Opgave 24
Anvend Euklids algoritme til at bestemme
a. sfd$(100, 101)$.
b. sfd$(123, 277)$.
c. sfd$(1529, 14039)$.
d. sfd$(11111, 111111)$.

Opgave 25
Hvor mange divisioner er det nødvendigt at foretage for ved hjælp af Euklids algoritme at bestemme:
a. sfd$(21, 34)$.
b. sfd$(34, 55)$.

Opgave 26
Med udgangspunkt i eksempel 2.18 opskriv da følgende største fællesdivisorer, dem fra opgave 24, på den i sætning 2.17 angivne form:
a. sfd$(100, 101)$.
b. sfd$(123, 277)$.
c. sfd$(1529, 14039)$.
d. sfd$(11111, 111111)$.

Opgave 27
Find primfaktoriseringen af følgende tal:
a. 39.
b. 126.
c. 143.
d. 1001.
e. 1013.
f. 1111.
g. 10! (bemærk, fakultet).

Opgave 28
Anvend sætning 2.29 (eller korollar 2.30) til at bestemme om følgende tal er primtal eller sammensatte tal:
a. 103.
b. 117.
c. 313.
d. 1013.
e. 1729.
f. 4013.
g. 5013.
h. 7717.

Opgave 29
Vis ved brug af induktion, at $n^3 - n$ er et deleligt med 3, når n er et positivt heltal.

Opgave 30
Vis ved brug af induktion, at summen af de første n lige positive heltal er $n(n+1)$.

Opgave 31
Vis at følgende Mersenne-tal enten er eller ikke er Mersenne-primtal:
a. $2^7 - 1$.
b. $2^9 - 1$.
c. $2^{11} - 1$.
d. $2^{13} - 1$.

3 Tre vigtige sætninger for RSA

Foruden de allerede sete elementer af talteorien hviler RSA-algoritmen (kapitel 4), eller nærmere bestemt korrektheden af denne, på tre matematiske sætninger: *Den kinesiske restsætning*, *Fermats lille sætning* og *Eulers sætning*. Vi skal løbende i dette kapitel stifte bekendtskab med de tre matematikere ansvarlige for disse talteoretiske resultater. Nærmere bestemt er der tale om den kinesiske matematiker Sun Zi, hvilket kan oversættes til mester Sun, som menes at have levet i det 5. århundrede, den franske 'hobby-matematiker' og af uddannelse jurist Pierre de Fermat, som levede i det 17. århundrede, og sidst men ikke mindst en af matematikkens allermest produktive mennesker schweizeren Leonhard Euler fra det 18. århundrede.

I de oprindelige fremstillinger af Sun Zi og Fermat anvendes ikke det der i dag er kendt som *modulo-regning*, eller med et andet ord *kongruenser*. Årsagen til dette er, at denne tilgang først for alvor blev en grundlæggende del af talteorien med den tyske matematiker Gauss i 1801. Kongruenser er imidlertid et fantastisk redskab når man har med heltal på flere hundrede cifre at gøre, som man har i RSA-kryptering. I dette kapitel vil samtlige af de talteoretiske resultater vi skal betragte derfor blive præsenteret i en (moderne) form anvendende kongruenser, ikke mindst fordi det er i denne form resultaterne blev brugt af folkene bag RSA. Vi begynder således med Gauss og hans formulering af kongruensbegrebet.

3.1 Kongruens

Ifølge matematikhistoriker Morris Kline begyndte der en ny æra inden for talteori med Gauss' publikation af *Disquisitiones Arithmeticae* (undersøgelser i aritmetik) i 1801. Gauss var påbegyndt dette arbejde mens han var studerende ved universitet i Göttingen og var i 1795 endt med at afbryde sine studier ved universitet for i stedet at forfølge sine egne ideer. To år senere, i en alder af 20, havde Gauss færdiggjort sit værk, men det tog ham yderligere fire år at få udgivelsen på plads. Som beskrevet i biografien ovenfor bidrog Gauss til adskillige områder inden for såvel matematik som fysik, men talteorien havde en særlig plads i Gauss' hjerte og han skal efter sigende have udtalt, at »Matematik er videnskabernes dronning, og talteori er matematikkens dronning.«

Gauss var på det tidspunkt, hvor han skrev *Arithmeticae* højst sandsynligt ikke bekendt med særlig mange af de dengang nyere resultater inden for talteori, hvilket han da også selv påpeger i sit forord:

> Mindst af alt må folk lade sig undre af at jeg næsten allerede i begyndelsen af bogen lægger ud med på ny at behandle mange resultater som har været aktivt studeret af andre. Jeg må forklare, at da jeg første gang kastede mig over denne type af undersøgelser i begyndelsen af 1795 ikke var bekendt med moderne opdagelser på området og havde ikke mulighed for at stifte bekendtskab med sådanne. [...] Da jeg omsider blev i stand til at studere arbejderne af disse genier [der hentydes her blandt andet til Fermat, Euler, Lagrange og Legendre] indså jeg at størstedelen af mine meditationer var blevet brugt på allerede veludviklede områder. [Alligevel] tillod jeg mig selv at blive overtalt til ikke at udelade nogle af de tidligere resultater, fordi der på daværende tidspunkt ikke var en bog som bragte arbejderne af tidligere geometere sammen, spredte som disse var blandt kommentarartikler i lærde akademier. Desuden var mange resultater nye, de fleste blev behandlet med nye metoder og de senere resultater hang så tæt sammen med de gamle, at de ikke kunne forklares uden at gentage fra begyndelsen. (Gauss; 1986, p. xviii-xix, oversat fra engelsk)

Selve ideen om modulo-regning og notationen af kongruenser kan ikke tilskrives Gauss – den findes allerede hos andre matematikere så som Euler og franskmændene Joseph-Louis Lagrange (1736-1813) og Adrien-Marie Legendre (1752-1833) – men det er i Gauss' *Arithmeticae* at begrebet for alvor viser sin styrke. Gauss begynder således på første linie i første kapitel af sit værk med at definere kongruenser, moduli og rester. Den moderne definition, tohundrede år senere, er stort set identisk med den af Gauss og brugen af $\equiv$-tegnet, som vi skal se anvendt nedenfor, skyldes da også netop Gauss.[1]

Carl Friedrich Gauss (1777-1855)

Carl Friedrich Gauss' skarpe intellekt og uhyre flair for matematik viste sig allerede i en tidlig alder og som 11-årig blev Gauss derfor sendt i gymnasiet i Brunswick. Som 15-årig begyndte Gauss på universitetet i Göttingen, men i 1795 afbrød han sine studier for at hellige sig sin egen forskning i blandt andet talteori. Fire år senere fik Gauss dog sin grad i Brunswick, hvor hertugen tilmed forlængede Gauss' stipendiat med en opfordring til Gauss om at indlevere en doktorafhandling til universitetet i Helmstedt. Det gjorde Gauss og afhandlingen var banebrydende idet den indeholdt et bevis for algebraens fundamentalsætning (enhver n'tegradsligning har n rødder i $\mathbb{C}$). I 1807 blev Gauss direktør for observatoriet i Göttingen og plejede i nogle år sin interesse for astronomi blandt andet med udgivelsen af et to-binds værk i 1809 om differentialligninger og himmellegemernes bevægelser. Gauss ydede også signifikante bidrag inden for differentialgeometri såvel som fysik og han regnes tilmed for at være den første der kendte til eksistensen af ikke-euklidisk geometri.

[1] Væsentlige dele af den matematiske fremstilling i dette kapitel er baseret på (Rosen; 2003).

Definition 3.1: Kongruens
Lad a, b og m være heltal med m større end nul. Heltallet a er kongruent med b modulo m, hvis $m \mid (a-b)$. Vi skriver $a \equiv b \pmod{m}$.

Bemærk, at hvis $a \equiv b \pmod{m}$ så vil der selvfølgelig også gælde, at $b \equiv a \pmod{m}$ (hvorfor?).

Eksempel 3.2
Da $6 \mid (17-5)$ haves ifølge definitionen, at $17 \equiv 5 \pmod{6}$. Da $6 \nmid (24-14)$ er 24 ikke kongruent med 14 modulo 6. ◇

En anden måde at tænke på kongruensbegrebet på er i termer af følgende sætning.

Sætning 3.3
Lad a, b, m være heltal med m større end nul. Da gælder, at $a \equiv b \pmod{m}$ hvis og kun hvis der findes et heltal k, således at $a = b + km$.

Bevis
At $a \equiv b \pmod{m}$ er ensbetydende med, at $m \mid (a-b)$, hvilket igen er ensbetydende med at der findes et heltal k således, at $a - b = km$, hvilket er det samme som $a = b + km$. Da de opskrevne udtryk i beviset alle er ensbetydende med hinanden gælder argumentet også 'baglæns' og vi har derfor bevist begge veje i hvis og kun hvis sætningen. □

Eksempel 3.4
Da der eksisterer et heltal $k = 2$ således, at $17 = 5 + 2 \cdot 6$ er $17 \equiv 5 \pmod{6}$. Da sætning 3.3 er en hvis og kun hvis sætning gælder argumentationen selvfølgelig også 'baglæns'. ◇

Og vi kan opstille en tredje måde at tænke på kongruensbegrebet på, også denne gang formuleret som en sætning.

Sætning 3.5
Lad a, b og m være heltal med m større end nul. $a \equiv b \pmod{m}$ hvis og kun hvis $a \pmod{m} = b \pmod{m}$.

Bevis *
Vi viser først den ene vej og derefter den anden. Antag således, at $a \equiv b \pmod{m}$, det vil sige at $a - b = km$ for et eller andet heltal k. Vi kan tage modulo m på dette udtryk, så længe vi bare gør det på begge sider af lighedstegnet:

$$(a-b) \pmod{m} = km \pmod{m}.$$

Ved at flytte modulo m ind i parentesen på venstresiden og udregne højresiden får vi, at

$$a \pmod{m} \; - b \pmod{m} = 0,$$

hvilket ved omrokering giver det ønskede resultat

$$a \pmod{m} = b \pmod{m}.$$

For den anden vej begynder vi med at antage, at $a(\mathrm{mod}m) = b(\mathrm{mod}m)$. Det vil sige at a og b har samme rest r ved division med m. Altså, at $a = q_1m + r$ og $b = q_2m + r$ for $0 \leq r \leq m$. Ved at trække b fra a får vi, at

$$\begin{aligned} a - b &= (q_1m + r) - (q_2m + r) \\ &= (q_1 - q_2)m. \end{aligned}$$

Men det betyder, at $m \mid (a-b)$, hvilket jo ifølge definitionen er det samme som, at $a \equiv b \,(\mathrm{mod}\, m)$. □

Eksempel 3.6
Da $17 \,(\mathrm{mod}\, 6) = 5 \,(\mathrm{mod}\, 6)$ er $17 \equiv 5 \,(\mathrm{mod}\, 6)$. Og omvendt. ◇

Vi burde nu have en ide om hvad kongruens er og hvad modulo-regning går ud på, så lad os nu vise en rigtig sætning om dette, ikke bare en 'omformulering' af definitionen.

Sætning 3.7
Lad m være et heltal større end nul. Hvis $a \equiv b \,(\mathrm{mod}\, m)$ og $c \equiv d \,(\mathrm{mod}\, m)$ så gælder, at

i. $a + c \equiv b + d \,(\mathrm{mod}\, m)$ *og*
ii. $ac \equiv bd \,(\mathrm{mod}\, m)$.

Bevis *
At $a \equiv b \,(\mathrm{mod}\, m)$ og $c \equiv d \,(\mathrm{mod}\, m)$ vil sige, at $a - b = ms$ og $c - d = mt$ for to heltal s og t.

I første tilfælde, (i), kan vi opskrive følgende:

$$\begin{aligned} (a + c) - (b + d) &= (a - b) + (c - d) \\ &= ms + mt \\ &= m(s + t). \end{aligned}$$

Men så vil $m \mid [(a + c) - (b + d)]$ og ifølge definitionen har vi da, at $a + c \equiv b + d \,(\mathrm{mod}\, m)$.

I det andet tilfælde, (ii), kan vi ræsonnere på lignende vis:

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= (a - b)c + b(c - d) \\ &= msc + bmt \\ &= m(sc + bt). \end{aligned}$$

hvorfor $m \mid (sc + bt)$ og $ac \equiv bd \,(\mathrm{mod}\, m)$. □

Eksempel 3.8
Vi betragter de to kongruenser $17 \equiv 5 \,(\mathrm{mod}\, 6)$ og $19 \equiv 1 \,(\mathrm{mod}\, 6)$. Ifølge sætning 3.7 (i) har vi, at

$$\begin{aligned} 17 + 19 \equiv 5 + 1 \,(\mathrm{mod}\, 6) &\Leftrightarrow 36 \equiv 6 \,(\mathrm{mod}\, 6) \\ &\Leftrightarrow 36 \equiv 0 \,(\mathrm{mod}\, 6), \end{aligned}$$

da $6 \mid 36$ med rest $r = 0$. Og ifølge sætning 3.7 (*ii*) har vi

$$17 \cdot 19 \equiv 5 \cdot 1 \pmod 6 \Leftrightarrow 323 \equiv 5 \pmod 6.$$

◇

En speciel type af kongruens, som Gauss også behandler i *Arithmeticae*, er hvad der i dag kendes som lineær kongruens.

Definition 3.9: Lineær kongruens
Lad a, b og m være heltal med $m \geq 1$. En kongruens af formen

$$ax \equiv b \pmod m,$$

hvor x er en variabel, kaldes for en lineær kongruens.

Et særtilfælde er når b i ovenstående definition er lig 1. De x'er der opfylde denne situation viser sig, hvilket vi senere skal få et indtryk af, at være særligt interessante, og har derfor sit eget navn.

Definition 3.10
Lad a og m være heltal med $m > 1$. Et heltal $\bar{a}$ der opfylder, at

$$\bar{a}a \equiv 1 \pmod m,$$

kaldes den inverse *af heltallet a modulo m.*

Eksempel 3.11
Bemærk, at -1 er en invers af 5 modulo 6, idet

$$-1 \cdot 5 \equiv 1 \pmod 6.$$

Bemærk endvidere, at -1 ikke er det eneste heltal der er en invers til 5 modulo 6, faktisk er det kun ét ud af følgende:

$$\ldots, -19, -13, -7, -1, 5, 11, 17, 23, \ldots$$

(Altså er ethvert heltal kongruent med -1 modulo 6 også en invers af 5 modulo 6.) ◇

Spørgsmålet er imidlertid, hvornår der eksisterer sådanne inverse. Sætning 3.13 giver et bud herpå, men først må vi have et lemma.

Lemma 3.12
Lad a, b, c og m være heltal med $m \geq 0$. Hvis $ac \equiv bc \pmod m$ og $\text{sfd}(c, m) = 1$ *da vil $a \equiv b \pmod m$.*

Bevis
At $ac \equiv bc \pmod m$ er ifølge definitionen det samme som, at $m \mid ac - bc = c(a - b)$. Da der endvidere gælder, at $\text{sfd}(c, m) = 1$ har vi ifølge sætning 2.19, at $m \mid a - b$, altså at $a \equiv b \pmod m$. □

Vi kan nu vise en sætning om under hvilke forudsætninger et heltal a i hvert fald har en invers $\bar{a}$.

Sætning 3.13
Lad a og $m > 1$ være heltal. Hvis a og m er indbyrdes primiske da gælder, at den inverse, $\bar{a}$, af a modulo m eksisterer og er entydigt fastlagt modulo m.

Med entydigt fastlagt modulo m forstås at der findes et entydigt positivt heltal $\bar{a} < m$ som er en invers af a modulo m og at enhver anden invers af a modulo m er kongruent med $\bar{a}$ modulo m (jævnfør eksempel 3.11). Vi skal som sætningen siger bevise såvel eksistens som entydighed.

Bevis
Vi begynder med eksistensen. Da $\text{sfd}(a, m) = 1$ findes der ifølge Bézouts identitet, sætning 2.17, heltal s og t således, at $sa + tm = 1$. Da $m > 1$ kan vi opskrive dette som $sa + tm \equiv 1 \pmod{m}$. Imidlertid har vi jo, at $tm \equiv 0 \pmod{m}$, hvorfor vi må have, at $sa \equiv 1 \pmod{m}$. Altså findes der et heltal s, således at dette er den inverse, $\bar{a}$, af a modulo m.

Og så entydigheden. Vi antager, at der findes to heltal s og t som hver især er indbyrdes primiske med a og som begge er inverse af a. Altså, at $sa \equiv 1 \pmod{m}$ og $ta \equiv 1 \pmod{m}$. Det vil sige, at $m \mid sa - 1$ og $m \mid ta - 1$. Hvis et tal går op i to andre tal, så går det også op i disse to tals differens, altså har vi at $m \mid (sa - 1) - (ta - 1) = sa - ta$. Dette er det samme som, at $sa \equiv ta \pmod{m}$. Det følger af lemma 3.12, at $s \equiv t \pmod{m}$, hvilket var det vi ønskede at vise. □

Vi ved fra eksempel 3.11, at -1 er en invers af 5 modulo 6. Men hvordan havde vi selv kunne finde den inverse af 5 modulo 6, hvis vi ikke på forhånd havde fået den givet? Følgende eksempel viser dette.

Eksempel 3.14
Med udgangspunkt i sætning 3.13 er det første vi kan bemærke, at der eksisterer en invers af 5 modulo 6, idet heltallene 5 og 6 er indbyrdes primiske, $\text{sfd}(5, 6) = 1$. Vi ved fra specialtilfældet af Bezouts identitet (se side 29), at når to heltal a og b er indbyrdes primiske, så kan de opskrives på formen $1 = sa + tb$. I vores tilfælde har vi

$$1 = s5 + t6.$$

Heltallene s og t kan bestemmes ved at gå 'baglæns' gennem Euklids algoritme. Men for at gøre dette må vi først gå forlæns, hvilket dog er nemt gjort da tallene er så små:

$$\begin{aligned} 6 &= 5 \cdot 1 + 1 \\ 5 &= 5 \cdot 1 + 0. \end{aligned}$$

Vi får, som vi skulle, at største fællesdivisor er 1, og ved at gå 'baglæns' får vi, at

$$1 = 1 \cdot 6 + (-1) \cdot 5.$$

Dette er imidlertid det samme som, at

$$-1 \cdot 5 \equiv 1 \pmod 6,$$

hvorfor -1 netop vil være en invers af 5 modulo 6. ◇

Når vi kender en invers $\bar{a}$ af a modulo m kan vi løse den lineære kongruens $ax \equiv b \pmod m$ ved at gange begge sider af kongruensen med $\bar{a}$. Lad os se hvordan.

Eksempel 3.15
Vi vil løse den lineære kongruens $5x \equiv 2 \pmod 6$. Fra eksempel 3.14 ved vi, at -1 er en invers til 5 modulo 6. Vi ganger derfor igennem med -1

$$-1 \cdot 5x \equiv -1 \cdot 2 \pmod 6.$$

Da $-5 \equiv 1 \pmod 6$ og $-2 \equiv 4 \pmod 6$ må der gælde, at hvis x er en løsning, så er $x \equiv -2 \equiv 4 \pmod 6$, altså $x \equiv 4 \pmod 6$. (Når dette er opfyldt vil løsningen som indsættes på x's plads 'gå ud med' højresiden af kongruensen, og $-5 \equiv 1 \pmod 6$ vil således stadig være opfyldt.)

Men er alle x med $x \equiv 4 \pmod 6$ så en løsning? Det er de faktisk og for at vise dette antager vi, at $x \equiv 4 \pmod 6$. Af sætning 3.7 (*ii*), med $5 \equiv 5 \pmod 6$ og $x \equiv 4 \pmod 6$, følger at

$$5 \cdot x \equiv 5 \cdot 4 \pmod 6 \quad \Leftrightarrow \quad 5x \equiv 20 \pmod 6 \quad \Leftrightarrow \quad 5x \equiv 2 \pmod 6,$$

hvilket viser at alle sådanne x'er opfylder kongruensen. Altså er løsningerne af denne type de følgende

$$\ldots, -20, -14, -8, -2, 4, 10, 16, 22, \ldots$$

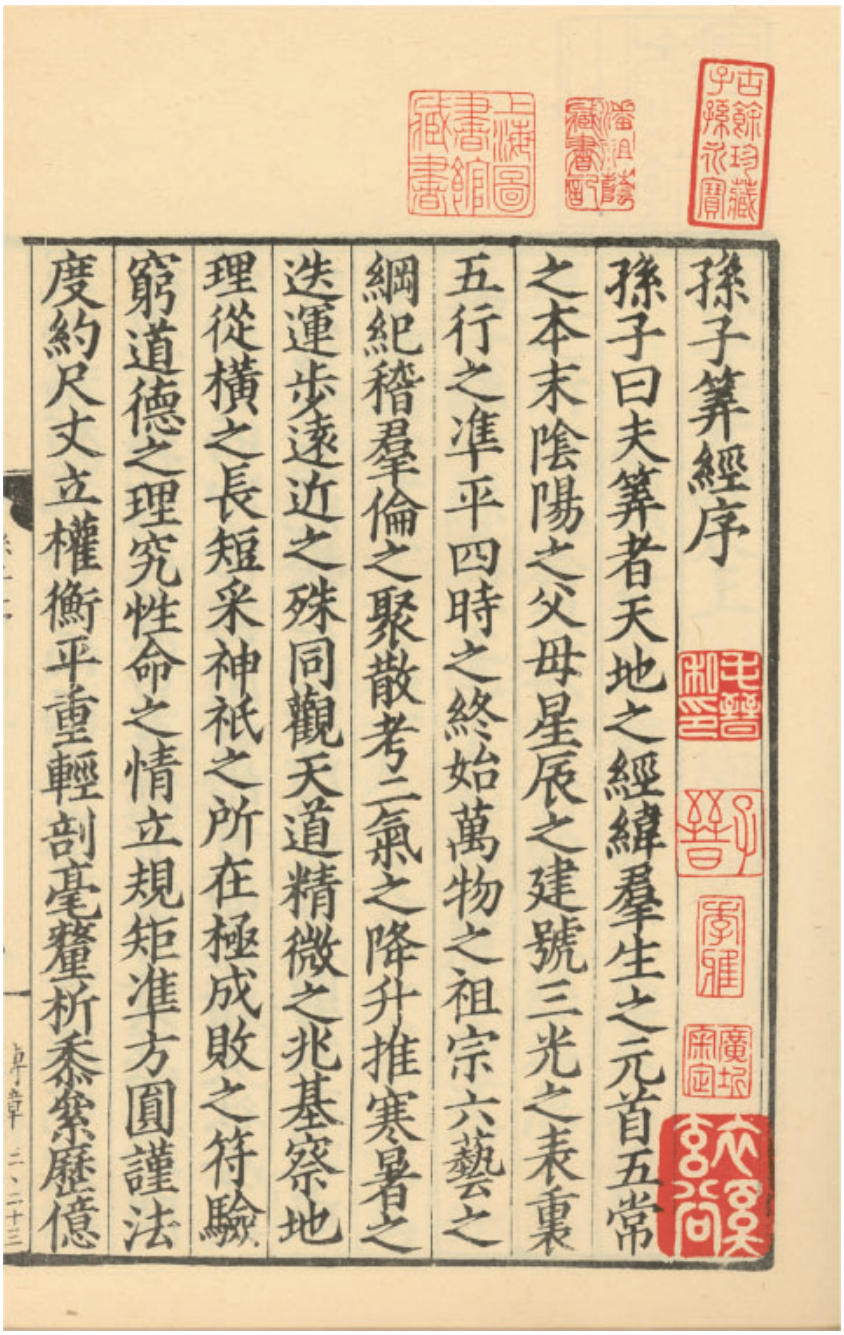
◇

Som vi skal se i det følgende afsnit spiller sætning 3.13 også en rolle i beviset for den kinesiske restsætning.

3.2 Den kinesiske restsætning

Der vides ikke meget om Sun Zi og hans gang på Jorden udover det skrift, *Sunzi suanjing* (Mester Suns matematiske manual), han har efterladt sig og som er gået i arv imellem de kinesiske herskere igennem århundreder. Som sagt menes Sun Zi at have levet i det 5. århundrede, men man er langt fra sikker. Studier af hans skrift tyder dog på, at dette tidligst kan dateres til år 280 og senest til år 473. Den bedste måde at danne sig et indtryk af Sun Zi på er nok ved at studere hans skrevne ord, og i særdeleshed forordet til skriftet.

> Mester Sun siger: Matematik styrer længden og bredden af himlene og Jorden; påvirker alle skabningers liv; former alfa og omega af de fem konstante dyder [gavmildhed, retfærdighed, sømmelighed, viden og oprigtighed]; agerer som forældrene af *yin* og


孫子算經序

孫子曰夫算者天地之經緯羣生之元首五常之本末陰陽之父母星辰之建號三光之表稟五行之準平四時之終始萬物之祖宗六藝之綱紀稽羣倫之聚散考二氣之降升推寒暑之迭運步遠近之殊同觀天道精微之兆基察地理從橫之長短采神祇之所在極成敗之符驗窮道德之理究性命之情立規矩準方圓謹法度約尺丈立權衡平重輕剖毫釐析黍案歷億

Figur 3.1 Forordet fra værket *Sunzi suanjing* som dateres til et sted mellem år 280 og år 473.

> *yang*; etablerer symboler for stjernerne og stjernebillederne; manifesterer dimensionerne af de tre lysende legemer [solen, månen og stjernerne]; opretholder balancen mellem de fem faser [metal, træ, vand, ild og jord]; regulerer begyndelsen og enden af de fire årstider; formulerer oprindelsen af en myriade af ting; og bestemmer principperne af de seks kunstarter [sømmelighed, musik, bueskydning, kørsel med stridsvogn, kalligrafi og matematik]. [...] Matematik har hersket i tusinder af år og er blevet brugt i stor udstrækning uden begrænsninger. Hvis man negligeer studiet af matematik vil man ikke være i stand til at opnå dygtighed og grundighed. Der er i sandhed en hel del at mestre når man betragter matematikken i perspektiv. Når man bliver interesseret i matematik vil man blive fuldt ud beriget; på den anden side, når man holder sig væk fra faget vil man opdage at man er intellektuelt indskrænket. Når man studerer matematik let som en ung mand med et åbent sind vil man øjeblikkeligt blive oplyst. Hvis man derimod nærmer sig matematikken som en gammel mand med en påståelig holdning vil man ikke blive dygtig deri. Ønsker man derfor at lære matematik på frugtbar vis må man disciplinere sig selv og stræbe efter perfekt koncentration; det er ad denne vej at succes i læring sikres. (Yong & Se; 1992, side 151-152, oversat fra engelsk)

Som sagt er den sætning fra Sun Zi som RSA-algoritmen gør brug af kendt som den kinesiske restsætning (for Sun Zis originale formulering af sætningen se opgave 45).

Til *vores* fremstilling af den kinesiske restsætning har vi brug for følgende lemma.

Lemma 3.16
Lad $m_1, m_2, \ldots, m_n$ være parvis indbyrdes primiske heltal større end 1. Hvis $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, n$, da er $a \equiv b \pmod{m}$, hvor $m = m_1 m_2 \cdots m_n$.

Bevis
At $a \equiv b \pmod{m_1 m_2 \cdots m_n}$ betyder jo, at

$$m_1 m_2 \cdots m_n \mid a - b,$$

så det er altså det vi skal vise. Lad os nu betragte primfaktoriseringerne af begge sider i dette udtryk. Antag, at p er et primtal der optræder i primfaktoriseringen af $m_1 m_2 \cdots m_n$. Ifølge lemma 2.25 har vi da, at $p \mid m_j$ for $1 \leq j \leq n$. Og i og med at m_i'erne ($1 \leq i \leq n$) er parvis indbyrdes primiske vil p udelukkende være en faktor i m_j. Da forudsætningen for at vores sætning gælder er, at $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, n$ har vi altså givet, at $m_j \mid a-b$. Fra sætning 2.3 (*iii*) ved vi da, at $p \mid a-b$ og tilmed må p optræde mindst lige så mange gange som faktor i $a-b$ som den gør som faktor i $m_1 m_2 \cdots m_n$. Men det vi så netop har vist er jo, at hver potens p^r i primfaktoriseringen af venstresiden, $m_1 m_2 \cdots m_n$, også optræder i primfaktoriseringen af højresiden, $a-b$. Derfor må $m_1 m_2 \cdots m_n \mid a-b$. □

Eksempel 3.17
Lad der være givet $m_1 = 2$, $m_2 = 3$, $m_3 = 5$ og $m_4 = 11$. Disse er alle primtal og derfor parvis indbyrdes primiske. Det bemærkes, at vi med $a = 331$ og $b = 1$ har, at $331 \equiv 1 (\mathrm{mod} 2)$, $331 \equiv 1 (\mathrm{mod} 3)$, $331 \equiv 1 (\mathrm{mod} 5)$ og $331 \equiv 1 \pmod{11}$. Ifølge sætning 3.16 har vi da, at $331 \equiv 1 \pmod{330}$, idet $2 \cdot 3 \cdot 5 \cdot 11 = 330$. ◇

Vi kan nu formulere og bevise den kinesiske restsætning.

Sætning 3.18: Den kinesiske restsætning
Lad $m_1, m_2, \ldots, m_n$ være parvis indbyrdes primiske positive heltal. Systemet

$$x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, \ldots, x \equiv a_n \pmod{m_n}$$

har en entydig løsning x modulo $m = m_1 m_2 \cdots m_n$.

Entydig løsning modulo m betyder igen, at der er en løsning x med $0 \leq x < m$ og at alle andre løsninger er kongruente modulo m til denne løsning. For at bevise den kinesiske restsætning må vi argumentere både for eksistensen af en løsning såvel som entydigheden af denne.

Bevis
Vi begynder med at vise eksistensen. For at konstruere en løsning x til systemet af de n kongruenser lader vi først

$$M_k = \frac{m}{m_k},$$

for $k = 1, 2, \ldots, n$. Det vil altså sige, at M_k er produktet af alle m_i'er på nær m_k. Da m_i og m_k $(1 \leq i, k \leq n)$ er indbyrdes primiske har de ingen fælles faktorer andre end 1 når $i \neq k$, hvorfor der også må gælde at $\mathrm{sfd}(m_k, M_k) = 1$. Fra sætning 3.13 ved vi, at der findes et heltal y_k som er en invers af M_k modulo m_k, altså $M_k y_k \equiv 1 \pmod{m_k}$. Vi danner nu summen

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n,$$

og viser dernæst, at denne sum er en løsning til systemet af kongruenser. Det første vi lægger mærke til er, at da $M_j \equiv 0 \pmod{m_k}$ når $j \neq k$, vil alle led på nær det k'te i summen være kongruente med 0 modulo m_k. Da $M_k y_k \equiv 1 \pmod{m_k}$ ser vi, at

$$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k},$$

for $k = 1, 2, \ldots, n$. Dermed har vi vist, at x er en løsning til systemet bestående af de n af kongruenser.

Entydigheden beviser vi på følgende vis: Vi antager, at der findes to forskellige løsninger, x og y, som begge er løsninger til systemet af de n kongruenser. Altså, at der for hvert i, $(1 \leq i \leq n)$, findes $x \equiv a_i \pmod{m_i}$ og $y \equiv a_i \pmod{m_i}$. Hvis vi kan vise, at disse løsninger er de samme modulo m har vi godtgjort at der kun findes én løsning x med $0 \leq x < m$.

Ved at sammenskrive udtrykkene for x og y ser vi, at der for hvert i, $(1 \leq i \leq n)$, må gælde, at $x \equiv y \pmod{m_i}$. Men af lemma 3.16 følger det da umiddelbart, at $x \equiv y \pmod{m}$, hvilket var det vi ønskede at vise. □

Bemærk, at eksistensdelen af beviset for den kinesiske restsætning i modsætning til beviset for aritmetikkens fundamentalsætning er et konstruktivt bevis. Det vil sige, at vi kan bruge konstruktionen anvendt i beviset til at løse et givet system af kongruenser. Lad os se et eksempel.

Eksempel 3.19
Lad der være givet systemet bestående af fire følgende ligninger:

$$x \equiv 1 \pmod{2},\ x \equiv 2 \pmod{3},\ x \equiv 3 \pmod{5},\ x \equiv 4 \pmod{11}$$

Da 2, 3, 5 og 11 alle er primtal og derfor parvis indbyrdes primiske kan vi benytte den kinesiske restsætning til at bestemme x, som vil være entydig modulo $m = m_1m_2m_3m_4 = 2 \cdot 3 \cdot 5 \cdot 11 = 330$. Vi beregner i overenstemmelse med notationen i beviset følgende:

$$M_1 = \frac{330}{2} = 165,\ M_2 = \frac{330}{3} = 110,\ M_3 = \frac{330}{5} = 66,\ M_4 = \frac{330}{11} = 30.$$

Det næste skridt er at bestemme de inverse y_i af M_i modulo m_i for $i = 1, 2, 3, 4$. Dette kan gøres forholdsvist let enten blot ved inspektion, da moduliene er forholdsvis små, eller ved mere systematisk brug af Euklids algoritme (jævnfør eksempel 3.14). Vi finder $y_1 = 1$, da $1 \cdot 165 \equiv 1 \pmod{2}$; $y_2 = 2$, da $2 \cdot 110 \equiv 1 \pmod{3}$; $y_3 = 1$ da $1 \cdot 66 \equiv 1 \pmod{5}$; og $y_4 = 7$, da $7 \cdot 30 \equiv 1 \pmod{11}$. Vores løsning er derfor

$$\begin{aligned} x &= a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4 \\ &= 1 \cdot 165 \cdot 1 + 2 \cdot 110 \cdot 2 + 3 \cdot 66 \cdot 1 + 4 \cdot 30 \cdot 7 \\ &= 1643 \\ &\equiv 323 \pmod{330}. \end{aligned}$$

Så løsningerne er altså af formen $323 + 330k$, hvor k er et heltal. ◇

3.3 Fermats lille sætning

I har måske hørt tale om Fermats sidste sætning, undertiden også omtalt som hans store sætning, der siger, at ligningen $x^n + y^n = z^n$ ingen ikke-trivielle heltalsløsninger har for $n > 2$. For $n = 2$ har ligningen uendeligt mange løsninger, de såkaldte Pytagoraiske tripler, eksempelvis $x = 3$, $y = 4$ og $z = 5$. Til trods for Fermats nedskriblede bemærkning i margin i hans oversatte udgave af den græske matematiker Diophantus' (cirka 200-284) *Arithmetica* – »Jeg har opdaget et i sandhed bemærkelsesværdigt bevis som denne margin er for lille til at rumme« – gik der over 350 år førend et bevis blev fundet. Sætningen blev endelig bevist af englænderen Andrew Wiles i 1995 og Wiles' bevis bygger i så høj grad på nyere matematik, at det i

hvert fald må anses for helt usandsynligt, at Fermat har kendt til netop dette bevis, som i øvrigt fylder 109 tætskrevne sider i et matematisk tidsskrift. Om Fermat derimod kendte til et andet bevis kan ikke vides med sikkerhed, og specielt ikke som Fermat havde for vane ikke at nedskrive særlig mange af sine beviser. Muligvis kendte Fermat allerede til sætningen i 1636, men betegnelsen 'sidste sætning' skyldes formentlig det faktum, at denne ikke blev offentlig kendt før i 1670, hvor hans søn Samuel udgav en udgave af Bachets oversættelse af Diophantus' *Arithmetica* indeholdende sin faders noter.

Den sætning som vi skal interesse os for her er den der i dag kendes som *Fermats lille sætning*. Fermat nævner første gang denne sætning i 1640, først i form af et par specialtilfælde i et brev til Mersenne i juni måned og senere i sin generelle form i et brev til en anden fransk 'hobby-matematiker', Bernard Frenicle de Bessy (1605-1675), i oktober måned. Fermat kom på sporet af sætningen i forbindelse med et spørgsmål (i forklædning) fra Frenicle angående, hvorvidt Mersenne-tallet $2^{37}-1$ er et primtal. Det mest interessante af specialtilfældene af den lille sætning i korrespondancen med Mersenne lyder:

> Hvis n er et primtal og p er en primdivisor i $2^n - 1$, så er $p - 1$ et multiplum af n.

Dette resultat brugte Fermat til at sige, at hvis $2^{37} - 1$ har en primdivisor p så må 37 gå op i $p - 1$. Fra et andet resultat vidste Fermat, at da p var ulige skulle det søges blandt primtallene af formen $74n + 1$. Det første primtal på denne form er 149, hvilket ikke er en divisor i $2^{37} - 1$, det næste er 223, hvilket rent faktisk viser sig at være en divisor, idet

$$2^{37} - 1 = 137438953471 = 223 \cdot 616318177,$$

hvorved Fermat havde vist, at $2^{37}-1$ ikke er et af de i dag såkaldte Mersenne-primtal.

Pierre de Fermat (1601-1665)

Pierre de Fermat var jurist af uddannelse og fra 1631 og frem til sin død fungerede han som byretsdommer i Toulouse i Frankrig, hvor han som en af sine juridiske bedrifter blandt andet fik brændt en præst på bålet. Men Fermat var også 'hobby-matematiker' og hans interesse for matematik menes at have begyndt under hans ophold i Bordeaux i slutningen af 1620'erne. Her mødte Fermat dommeren Étienne d'Espagnet og fik gennem ham adgang til flere af Viètes matematiske værker. Gennem sin kollega og ven, Pierre de Carcavi (1600-1684), blev Fermat i 1636 introduceret til en gruppe bestående af matematikerne Mersenne, Étienne Pascal (1588-1651) og Roberval (1602-1675). Det var gennem korrespondancer med dem, og specielt via munken Mersenne til andre matematikere, at Fermat kunne pleje sin interesse for matematikken. Fermat lavede i sin levetid banebrydende arbejde inden for talteori, udviklede sandsynlighedsregningen sammen med Étiennes søn Blaise Pascal (1623-1662), etablerede differentialregningen og meget mere.

Til vores moderne fremstilling af Fermats lille sætning bliver vi nødt til at have en håndfuld andre sætninger på banen først. Men som vi skal se vil vi i beviserne for disse heldigvis ofte kunne støtte os til en del af de resultater vi allerede har vist i de foregående afsnit. Mere præcist skal vi basere vores bevis for Fermats lille sætning på en anden sætning kendt som Wilsons sætning og for at bevise denne har vi brug for to lemmaer.

Lemma 3.20
Lad p være et primtal. De eneste løsninger x til ligningen

$$x^2 \equiv 1 \pmod{p}$$

er de der opfylder ligningerne $x \equiv 1 \pmod{p}$ og $x \equiv -1 \pmod{p}$.

Bevis
At heltal x er løsninger til $x^2 \equiv 1 \pmod{p}$ vil sige, at $p \mid x^2 - 1$. Men da $(x^2 - 1) = (x + 1)(x - 1)$ er vi altså ude efter x'er for hvilke der gælder, at $p \mid (x + 1)(x - 1)$. Fra lemma 2.25 ved vi, at dette kun er tilfældet, hvis enten $p \mid x + 1$ eller $p \mid x - 1$. Men det er jo det samme som at $x \equiv 1 \pmod{p}$ eller $x \equiv -1 \pmod{p}$. □

Værd at bemærke i denne sammenhæng er, at $-1 \pmod{p}$ jo er det samme som $p - 1 \pmod{p}$. Vi skal bruge dette i beviset for det næste lemma.

Lemma 3.21
Hvis p er et primtal gælder der, at de positive heltal r, $1 < r < p - 1$, kan splittes op i $(p - 3)/2$ par af heltal, således at hvert par består af hinandens inverse modulo p.

Bevis
Vi bemærker først, at alle positive heltal $r < p$ nødvendigvis må være indbyrdes primiske med p, da p jo er et primtal og derfor ikke har andre divisorer end 1 og sig selv. Af sætning 3.13 følger da, at alle positive heltal $r < p$ har en invers modulo p og at denne inverse er entydig blandt heltallene $r < p$. Når alle heltal $r < p$ på denne måde har en entydig invers må vi kunne inddele disse i par bestående af et heltal og dets inverse. Det eneste mulige problem er, hvis et heltal er sit eget inverse, i hvilket tilfælde vi ikke får et par. Ifølge lemma 3.20 er det dog kun heltallene 1 og -1 (det vil sige $p - 1$) der er deres egne inverse modulo p. Derfor kan alle positive heltal r med $1 < r < p - 1$ altså grupperes i par bestående af to heltal som er hinandens inverse. Og der findes netop $(p - 1 - 2)/2 = (p - 3)/2$. □

Nu kan vi så vise den såkaldte Wilsons sætning, opkaldt efter den engelske matematiker John Wilson (1741-1793) som fandt sætningen omkring 1760. Matematikhistoriske studier har dog senere vist, at den tyske matematiker Gottfried Wilhelm von Leibniz (1646-1716) kendte resultatet allerede i 1683. Imidlertid publicerede Leibniz ikke noget derom, og det gjorde Wilson faktisk heller ikke. Første gang sætningen så dagens lys var da en anden engelsk matematiker, Edward Waring (1736-1798), publicerede den, men med reference til

Wilson. Værd at bemærke er at hverken Wilson eller Waring beviste resultatet, det blev først gjort af den franske matematiker Joseph-Louis Lagrange i 1771. Det følgende bevis er dog ikke Lagranges, men derimod et nyere et.

Sætning 3.22: Wilsons sætning
Hvis p er et primtal gælder der, at $(p-1)! \equiv -1 \pmod{p}$. (Bemærk fakulteten.)

Bevis
For at udregne

$$(p-1)! = 1 \cdot 2 \cdots (p-2) \cdot (p-1)$$

kan vi gruppere produktet på højresiden i par af heltal som er hinandens inverse. At vi kan dele højresiden op i par følger af, at p er et primtal og derfor ulige (for $p > 2$), hvorfor $p-1$ er et lige tal og fakultet af et lige tal er et produkt af et lige antal tal. Da hvert sådant par giver anledning til produktet 1 modulo p vil det samlede produkt modulo p være lig produktet af de eneste uparrede elementer, nemlig 1 og $p-1$, altså $1 \cdot (p-1) = p-1$. Og da $p-1 \pmod{p}$ er det samme som $-1 \pmod{p}$ har vi vist Wilsons sætning. □

Eksempel 3.23
Lad os betragte primtallet 5. Vi har, at $(5-1)! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$ og ganske rigtigt gælder, at $24 \equiv -1 \pmod{5}$. ◇

Ofte er det nyttigt at have Wilsons sætning på en anden form, nemlig den af følgende korollar, og faktisk var Lagranges bevis for Wilsons sætning i 1771 netop et bevis for denne version af sætningen.

Korollar 3.24
Hvis $(n-1)!$ *ikke er kongruent med* -1 *modulo* n*, så er* n *ikke et primtal.*

Nu hvor vi har Wilsons sætning i baghånden er vi i stand til bevise Fermats lille sætning, så lad os se hvad denne siger.

Sætning 3.25: Fermats lille sætning
Hvis p er et primtal og n er et vilkårligt heltal, hvorom det gælder at $p \nmid n$, så er

$$n^{p-1} \equiv 1 \pmod{p}.$$

Bevis
Beviset for Fermats lille sætning kan for overskuelighedens skyld opdeles i tre dele.

(1) Lad der være givet heltallet n, hvorom gælder at $p \nmid n$. Vi skal begynde med, at argumentere for at ingen to heltal

$$1n, 2n, 3n, \ldots, (p-1)n$$

er kongruente modulo p. Dette argumenterer vi for ved en modstrid. Antag derfor, at der er to sådanne heltal, in og jn for $1 \leq i < j < p$,

som er kongruente modulo p, $in \equiv jn \pmod{p}$, hvilket er det samme som, at $p \mid jn - in$, eller $p \mid (j-i)n$. Da n og p er indbyrdes primiske og $p \mid (j-i)n$ følger af sætning 2.19 at $p \mid (j-i)$ (vi har jo, at $p \nmid n$). Men dette er jo umuligt siden $j - i$ nødvendigvis er et positivt heltal mindre end p, altså har vi en modstrid.

(2) Da vi ifølge ovenstående har at ingen to heltal $1n, 2n, 3n, \ldots, (p-1)n$ er kongruente modulo p må det forholde sig således, at hvert af disse heltal er kongruent modulo p til et forskelligt tal mellem 1 og $p-1$. Tager vi derfor produktet $1n \cdot 2n \cdot 3n \cdots (p-1)n$ modulo p vil resultatet af dette være det samme som produktet af tallene fra 1 til $p-1$ modulo p, altså

$$1n \cdot 2n \cdot 3n \cdots (p-1)n \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

hvilket vi kan omskrive til

$$(p-1)!n^{p-1} \equiv (p-1)! \pmod{p}.$$

(3) Ifølge Wilsons sætning, sætning 3.22, er $(p-1)! \equiv -1 \pmod{p}$, hvorfor vi kan omskrive ovenstående udtryk til

$$(-1)n^{p-1} \equiv -1 \pmod{p}.$$

Ved at gange igennem med -1 får vi det ønskede resultat,

$$n^{p-1} \equiv 1 \pmod{p},$$

og da vi allerede i del (1) af beviset forudsatte, at $p \nmid n$ har vi altså Fermats lille sætning. □

Eksempel 3.26
Lad igen $p = 5$ og lad $n = 6$, der gælder at $5 \nmid 6$. Vi har at $6^{5-1} = 6^4 = 1296$. Der gælder oplagt at 5 er en divisor i 1295, hvorfor $6^{5-1} \equiv 1 \pmod{5}$. ◇

En anden formulering af Fermats lille sætning, som man også tit støder på, lyder:

Sætning 3.27
Lad p være et primtal, da haves for alle heltal n, at

$$n^p \equiv n \pmod{p}.$$

Bevis
For at vise dette må vi kigge på to tilfælde: $p \mid n$ og $p \nmid n$. Hvis $p \nmid n$ ganger vi blot igennem med n i udtrykket fra sætning 3.25 og får således det ønskede. Hvis $p \mid n$ så vil begge sider af $n^p \equiv n \pmod{p}$ være 0 modulo p og kongruensen vil derfor stadig være sand. □

En hel del af Fermats andre interesseområder, som for eksempel sandsynlighedsregningen, kunne han diskutere med ligesindede matematikere. Med talteorien var det imidlertid en anden sag, da der kun var få af Fermats samtidige matematikere, udover Frenicle og Mersenne, der havde interesse i denne. Fermat overvejede i flere omgange selv at publicere et værk indeholdende sine talteoretiske resultater, men at sende noget i pressen på Fermats tid var langtfra en nem sag for en matematiker. For at typografen kunne udføre et tåleligt stykke arbejde måtte han nøje superviseres af enten forfatteren selv eller en anden som var bekendt med forfatterens stil og notation. Da Fermat ikke kunne finde nogen som ville påtage sig dette job, og da han ikke selv følte sig i stand dertil, opgav han at publicere. Således var det ikke førend i 1670, da Samuel de Fermat begyndte at udgive sin faders efterladte skrifter, at Fermats arbejde med talteori blev offentlig kendt. Men da ingen af 1600-tallets matematikere interesserede sig for talteori fik offentliggørelsen ikke nogen større betydning til at begynde med. Ikke før i midten af det 18. århundrede blev tråden samlet op af en anden matematiker, hvis interessesfære inden for matematikken, ligesom Fermats, bredte sig vidt. Denne matematiker var Leonhard Euler.

3.4 Eulers sætning

I 1600-tallet var det at være matematiker oftest en fritidsbeskæftigelse, da der ikke var særlig mange faste stillinger ved akademierne rundt omkring i Europa. Store matematikere som Viète, Fermat og Leibniz var derfor såkaldte 'hobbymatematikere', der drev deres matematiske virksomhed, omend for disse tre på et meget højt niveau, ved siden af deres faste stillinger. Viète var uddannet jurist, men besad igennem sin levetid diverse forskellige stillinger, eksempelvis i parlamentet i Paris som privat kongelig rådgiver for Henrik III samt som kryptoanalytiker; som vi ved var Fermat af uddannelse ligeledes

Leonhard Euler (1707-1783)

Leonhard Euler er en af de mest producerende og formentlig også største matematikere gennem tiden. I en alder af 14 år begyndte han på universitet i Basel, hvor han snart blev opdaget af matematikprofessoren Johann Bernoulli. Eulers far, der var præst, havde selv studeret en smule matematik under Johanns ældre bror, Jacob, og gik med til at hans søn læste matematik i stedet for teologi, hvilket ellers var planen. Euler færdiggjorde sine studier som 19-årig. I 1727 blev Euler ansat ved akademiet i Skt. Petersborg og forblev tilknyttet hertil resten af sit liv til trods for et 25-årigt ophold i Berlin fra 1741-1766. Fra 1766 og frem til sin død i 1783 opholdt Euler sig sammen med sin kone og fem børn i Sct. Petersborg. Som følge af en sygdom mistede Euler i 1738 synet på sit højre øje og synet på det venstre blev gradvist svagere frem til 1771, hvor han var helt blind. Til trods for blindheden producerede Euler næsten halvdelen af sit enorme arbejde, i såvel matematik som fysik, i perioden efter 1765 blandt andet med hjælp fra sine to ældste sønner.

jurist og af profession dommer; og også Leibniz var uddannet inden for jura og besad gennem det meste af sit liv stillinger ved domstolene. En af de mere ekstreme historier er den om Johann Bernoulli (1667-1748), hvis ældre bror Jacob Bernoulli (1654-1705) var professor i deres hjemby Basel, hvilket ikke efterlod meget håb for Johann om at få job samme sted. Inden Johann selv blev professor i Groningen så han sig således nødsaget til at tage et job, hvor han underviste den franske adelsmand Marquis de l'Hôspital i Leibniz' infinitesimalregning. I kontrakten mellem de to indgik tilmed at Johann Bernoulli skulle overlade alle sine matematiske resultater til l'Hôspital. Marquis de l'Hôspital finansierede senere selv udgivelsen af en bog i sit eget navn indeholdende Bernoullis resultater.

Situationen som de her ovennævnte matematikere befandt sig i stillede visse krav, hvis de ville vide hvad der rørte på sig rundt omkring i Europa. De måtte være en del af et solidt netværk, som vi så det med Fermat og hans brevkorrespondancer gennem Mersenne, og det var næsten en nødvendighed at have et hjemmebibliotek af en anseelig størrelse. Fra starten af 1700-tallet begyndte billedet at ændre sig, hvilket skyldtes etablereringen af mere eller mindre videnskabelige samfund, for eksempel naturvidenskabelige akademier, og dertil hørende publikationsmuligheder. Situationen begyndte altså i højere grad at ligne den vi kender fra universiteterne i dag. Så da Euler som 19-årig i 1726 stod parat til at træde ind på matematikkens scene var omstændighederne ganske anderledes end de havde været det for Fermat små hundrede år forinden.

Eulers interesse for talteori blev vakt da han gennem sine venner og kollegaer brødrene Nicolas og Daniel Bernoulli, sønner af Eulers gamle læremester Johann Bernoulli, blev introduceret for Christian Goldbach (1690-1764). Goldbach var en lærd preusser som havde slået sig ned i Rusland, hvor han besad forskellige poster ved den russiske stat. Goldbach er i dag mest kendt for en formodning omhandlende primtal – en formodning som stadig hverken er be- eller afvist – men den skal vi vende tilbage til i afsnit 3.5. Goldbachs interesser som matematiker kredsede sig udover differentialregning og talrækker ikke mindst om talteorien, og det er derfor ikke så mærkeligt at Goldbach allerede i den første brevveksling med Euler henledte dennes opmærksomhed på emnet. I året 1729 skrev Goldbach således til den unge Euler: »Er Fermats formodning dig bekendt, at alle tal af formen $2^{2^n}+1$ er primtal? Han [Fermat] sagde, at han ikke kunne bevise det; og ligeledes har ingen andre kunnet, så vidt jeg ved.« I begyndelsen lod Euler sig ikke imponere af Goldbachs forsøg på at bringe talteori på banen, hvilket måske ikke er så overraskende. Talteori var på dette tidspunkt stadig ikke en særlig populær disciplin inden for matematikken, faktisk blev den af mange nærmest betragtet som en kuriositet, og derfor havde den heller ikke været en del af den uddannelse som Euler havde modtaget af Johann Bernoulli. Men Goldbach insisterede, og i juni 1730 bed Euler på krogen. Han tog nu emnet alvorligt og begyndte tilmed at studere de af Fermats skrifter som han kunne få fat på. Goldbach selv havde faktisk aldrig læst Fermat, hvilket han senere fortalte Euler, men Fermats formodninger og påstande synes at have cirkuleret blandt talentusiaster som en form for sagn og myter, og specielt Fermats 'sidste sætning' var velkendt.

Det var Goldbachs omtale af den ovennævnte formodning af Fermat som satte Euler på sporet af Fermats lille sætning. Formentlig opdagede og viste Euler allerede Fermats lille sætning såvel som generaliseringen af den, Eulers egen sætning, i 1735-36, og dette uden at kende til Fermats formulering af sætningen i forvejen. Faktisk menes det ikke at Euler fik adgang til de af Fermats skrifter, hvori sætningen nævnes førend flere år senere. Men lad os se hvorledes Eulers generalisering af Fermats lille sætning, fundet omtrent hundrede år efter at den lille sætning så dagen lys første gang, ser ud.

For at forstå Eulers sætning må vi først have en definition på banen, nemlig definitionen af Eulers ϕ-funktion (det græske bogstav phi).

Definition 3.28: Eulers ϕ-funktion
For hvert heltal m større end eller lig 1 angiver $\phi(m)$ antallet af heltal r, med $1 \leq r < m$, således at r er indbyrdes primisk med m, altså $\text{sfd}(r, m) = 1$. *$\phi(m)$ kaldes for* Eulers ϕ-funktion.

Eksempel 3.29
$\phi(15)$ er altså antallet af positive heltal mindre end 15, som er indbyrdes primiske med 15. Disse heltal er netop tallene 1,2,4,7,8,11,13,14, da den største fællesdivisor af disse tal og 15 er 1. Altså er $\phi(15) = 8$.

$\phi(17) = 16$ da samtlige tal fra 1-16 er indbyrdes primiske med 17. $\diamond$

At ϕ-funktionen af et primtal er netop én mindre en primtallet selv, som i tilfældet med 17 i ovenstående eksempel, er ingen tilfældighed, hvilket følgende sætning viser.

Sætning 3.30
Lad p og q være to forskellige primtal og lad $n = pq$. Da gælder, at

i. $\phi(p) = p - 1$.

ii. $\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1)$.

Bevis
Vi beviser først (*i*) og derefter (*ii*).

(*i*) Siden p er et primtal, og det derfor kun er tallene 1 og p selv der er divisorer heri, vil der netop være $p - 1$ heltal mindre end p som er indbyrdes primiske med p (heltallet 1 er jo også indbyrdes primisk med p). Det vil sige, at $\phi(p) = p - 1$.

(*ii*) Denne del kræver en smule mere udredning end den første, omend beviset i bund og grund kun er et 'regnestykke'. Da p og q er (forskellige) primtal og $n = pq$ har n ikke andre primfaktorer end disse. Alle heltal $s < n$ der *ikke* er indbyrdes primiske med n kan derfor skrives som mængden (jævnfør eventuelt beviset for Fermats lille sætning):

$$S = \{1p, 2p, \ldots, (q-1)p\} \cup \{1q, 2q, \ldots, (p-1)q\}.$$

Antallet af elementer i mængden S er $(p - 1) + (q - 1) = p + q - 2$. Da jo $n = pq$ er der i alt $pq - 1$ positive heltal mindre end n. Antallet af

positive heltal indbyrdes primiske med $n = pq$, det vil sige $\phi(n)$, må da være givet ved:

$$\begin{aligned}\phi(n) &= (pq-1)-(p+q-2)\\ &= pq-p-q+1\\ &= (p-1)(q-1)\\ &= \phi(p)\phi(q).\end{aligned}$$

□

Eksempel 3.31
Lad os igen kigge på heltallet 15. 15 kan faktoriseres op i produktet af de to primtal 3 og 5. Altså har vi ifølge sætning 3.30 (*ii*), at

$$\phi(15) = \phi(3)\phi(5) = (3-1)(5-1) = 2\cdot 4 = 8,$$

hvilket også stemmer overens med forrige eksempel. ◇

Vi er nu klar til at formulere og bevise Eulers sætning.

Sætning 3.32: Eulers sætning
Lad n være indbyrdes primisk med m. Da gælder, at

$$n^{\phi(m)} \equiv 1 \pmod{m}.$$

Bevis
Ligesom i beviset for Fermats lille sætning betragter vi en følge af heltal, nærmere bestemt de $\phi(m)$ heltal r_i der er indbyrdes primiske med m:

$$r_1, r_2, r_3, \ldots, r_{\phi(m)}.$$

Disse ganger vi nu hver især med n:

$$nr_1, nr_2, nr_3, \ldots, nr_{\phi(m)}.$$

Bemærk, at denne følge enten er en delfølge af følgen fra beviset for Fermats lille sætning eller, i det tilfælde hvor m er et primtal, er lig denne følge. Den kan altså ikke være mere omfattende. Da vi endvidere har at $m \nmid n$ (m og n er indbyrdes primiske) befinder vi os i samme situation som i beviset for Fermats lille sætning og kan ved brug af samme argumenter opskrive følgende sande udtryk:

$$nr_1 \cdot nr_2 \cdot nr_3 \cdots nr_{\phi(m)} \equiv r_1 \cdot r_2 \cdot r_3 \cdots r_{\phi(m)} \pmod{m}.$$

Dette kan vi omskrive til

$$n^{\phi(m)}(r_1 \cdot r_2 \cdot r_3 \cdots r_{\phi(m)}) \equiv r_1 \cdot r_2 \cdot r_3 \cdots r_{\phi(m)} \pmod{m}.$$

Da alle r_i'erne, $1 \leq i \leq \phi(m)$, er indbyrdes primiske med m kan vi forkorte dem bort og få, at

$$n^{\phi(m)} \equiv 1 \pmod{m},$$

hvilket var det vi skulle vise. □

Som sagt er Eulers sætning en generalisering af Fermats lille sætning. Dette ses forholdsvist let ved at lade m'et i Eulers sætning være et primtal p. Et primtal p vil selvfølgelig også være indbyrdes primisk med et givet heltal n og ifølge det foregående ved vi, at Eulers ϕ-funktion af et primtal p er lig $p-1$. Indsættelse af disse værdier giver os præcist Fermats lille sætning:

$$n^{\phi(p)} \equiv 1 \pmod{p} \Leftrightarrow n^{p-1} \equiv 1 \pmod{p}.$$

Med andre ord er Fermats lille sætning altså et specialtilfælde af Eulers sætning. Vi kan efterprøve dette med et lille eksempel.

Eksempel 3.33
Lad $m = 5$ og $n = 6$. Da 5 og 6 er indbyrdes primiske, sfd$(5, 6) = 1$, kan vi benytte Eulers sætning. $\phi(5) = 4$, hvorfor vi har at $6^4 \equiv 1 \pmod{5}$. Da 5 udover at være et heltal faktisk også er et primtal kan vi opnå samme resultat ved brug af Fermats lille sætning. Og rent faktisk var det det vi gjorde i eksempel 3.26. ◇

Ved hjælp af Eulers sætning skal vi vise endnu en lille sætning, et korollar som vi i kapitel 4 skal bruge i beviset for korrektheden af RSA-algoritmen.

Korollar 3.34
Lad n og m være indbyrdes primiske heltal og lad t være et vilkårligt heltal. Da gælder, at

$$n^t \equiv n^{t \pmod{\phi(m)}} \pmod{m}.$$

Bevis *
Sætningen siger altså, at man kan tage modulo $\phi(m)$ af eksponenten t. For at vise dette vil vi begynde med at foretage følgende omskrivning af heltallet n^t:

$$n^t = n^{t-k\cdot\phi(m)+k\cdot\phi(m)},$$

hvor vi lader k være givet på en sådan vis, at det at fratrække $k \cdot \phi(m)$ svarer til at regne modulo $\phi(m)$. Vi forsætter omskrivningen:

$$\begin{aligned} n^t &= n^{t \pmod{\phi(m)}+k\cdot\phi(m)} \\ &= n^{t \pmod{\phi(m)}} \cdot n^{k\cdot\phi(m)} \\ &= n^{t \pmod{\phi(m)}} \cdot n^{(\phi(m))^k}. \end{aligned}$$

Ifølge Eulers sætning har vi nu, at

$$n^{t \pmod{\phi(m)}} \cdot n^{(\phi(m))^k} \equiv n^{t \pmod{\phi(m)}} \cdot 1^k \pmod{m}.$$

Da 1^k på venstre-siden er lig 1 og da højre-siden jo er konstrueret således, at den er lig n^t får vi det ønskede resultat:

$$n^t \equiv n^{t \pmod{\phi(m)}} \pmod{m}.$$

□

Eksempel 3.35
Lad igen $n = 6$ og $m = 5$ og lad os sætte $t = 9$. Korollaret siger nu, at

$$\begin{aligned} 6^9 &\equiv 6^{9 \pmod{\phi(5)}} \pmod 5 \\ &\equiv 6^{9 \pmod 4} \pmod 5 \\ &\equiv 6^1 \pmod 5. \end{aligned}$$

$6^9 = 10077696$ modulo 5 er oplagt lig 1 og det samme er 6 modulo 5. $\diamond$

Euler forsatte sit arbejde med talteorien og i 1748 – samme år som det formodes Euler første gang fik fat i en kopi af 1670-udgaven af Diophantus' *Arithmetica* indeholdende Fermats kommentarer – gik Euler igang med at forfatte et større værk om talteori, men projektet strandede. Euler nåede i alt at skrive seksten kapitler førend han opgav projektet. Kapitlerne blev ikke udgivet førend i 1849, mere end halvtreds år efter Eulers død, under titlen *Tractatus de numerorum doctrina*. Det interessante ved Eulers denne 'introduktion' til talteori er imidlertid, at disse kapitler i høj grad minder om Gauss' første udkast til de indledende dele af hans *Disquisitiones Arithmeticae* fra 1801. Eksempelvis behandlede Euler her såvel kongruens som lineær kongruens inden han præsenterede sin generalisering af Fermats lille sætning. Faktisk bestod en hel del af Eulers arbejde med talteorien i at bevise flere af de formodninger og formulerede sætninger som Fermat havde givet uden bevis. Euler fortsatte i hele denne periode såvel som efter med at søge efter Fermats (forsvundne) skrifter. Allerede i 1742 havde Euler forsøgt at iværksætte en søgen, men ingen andre matematikere syntes på det tidspunkt interesserede nok i Fermats talteori til at medvirke i en sådan eftersøgning, hverken i Paris eller andre steder. Euler måtte derfor gøre det selv, hvilket han gjorde med Lagranges uvurderlige hjælp fra 1768 og fremefter. Da Euler døde i 1783 var det terræn som Fermat havde inddraget atter genvundet af Euler og nyt var føjet til.

Lagrange var sammen med Legendre en af de få arvtagere til Eulers og Fermats talteori. Lagrange havde skrevet sit første brev til Euler i 1754, et brev som Euler ikke havde fundet interessant nok til at besvare. Men året efter skrev Lagrange et nyt og denne gang et som lod til at imponere Euler, i hvert fald behandlede Euler fra dette tidspunkt af altid den væsentlig yngre Lagrange som en ligeværdig. Lagrange omtaler da også Euler som »den eneste kompetente dommer i talteoretiske spørgsmål« idet det ifølge Lagrange kun er Fermat og Euler der på dette tidspunkt har haft succes i sådanne henseender. Tilmed påpeger han, at i fald han selv har været så heldig at kunne føje til Eulers opdagelser, så skyldes det intet andet end de studier han har gjort af Eulers excellente arbejder. En ting er dog Lagranges og Legendres syn på talteori, noget andet er andre matematikeres. Attituden hos matematikere generelt set var nemlig ikke stort ændret, og det på trods af at en af de største af dem alle, Euler, var en så varm fortaler for emnet. I 1778, fem år før Eulers død, sendte en af Eulers elever nogle af sin mesters resultater omhandlende primtal til Nicholas Bernoulli. Denne svarede:

> Hvad du har taget dig tid til at fortælle mig om dette spørgsmål forekommer mig såvel opfindsomt som vores store mester [Euler]

> værdigt. Men, jeg beder, er det næsten ikke at gøre primtallene for stor ære at sprede sådanne rigdomme over dem, og skylder man ikke at vise ærbødighed til al den finesse vores tid byder på? [Nu til Euler:] Jeg respekterer alt, hvad der kommer fra din pen og beundrer din store evne til at overkomme selv de mest vanskelige problemer; men min beundring fordobles, hvis emnet leder til brugbare områder af viden. Dette inkluderer, efter min mening, dine dybe undersøgelser af bjælkers styrke... (Weil; 1984, side 224)

Som allerede påpeget trådte talteorien dog ind i en ny æra med udgivelsen af Gauss' *Disquisitiones Arithmeticae* i 1801. Dette skal vi se lidt nærmere på i næste afsnit, hvor vi også skal præsenteres for et udvalg af talteoriens uløste gåder.

3.5 Uløste problemer i talteori

Der findes inden for talteorien et hav af gåder, uløste problemer, formodninger, postulater og hypoteser. Faktisk er der så mange at der er skrevet bøger udelukkende derom, for eksempel (Guy; 1994). Vi skal i dette afsnit se på nogle af de mest berømte af disse.

Et af de helt centrale problemer består i, hvordan man kan bestemme om et tal er et primtal eller ej. En mulighed er selvfølgelig at begynde at regne, det vil sige forsøge at faktorisere det givne heltal på lignende vis som vi så det i kapitel 2. Imidlertid er denne metode tidskrævende og jo større de givne tal bliver jo mere uoverskuelige bliver udregningerne. Det er så selvfølgelig oplagt at benytte sig af tekniske hjælpemidler til beregningerne, hvilket gennem historien også er blevet gjort i stor stil. Før computerne blev introduceret byggede man mekaniske maskiner, hvis formål var at primfaktorisere store heltal. Et eksempel på en sådan maskine var den bygget af den amerikanske matematiker Derrick Norman Lehmer (1867-1938) i 1926. Maskinen bestod af en savbuk, en række cykelkæder med indsatte bolte, en elektromotor som drev maskinen samt andre forhåndenværende materialer. Boltene blev benyttet til at programmere maskinen med det problem man ønskede at løse, elektromaskinen drev derefter maskinen i sin sindrige søgning af faktorerne, og når motoren stoppede kunne man på kombinationen af bolte i kæderne aflæse svaret. Eksempelvis fandt Lehmer ved brug af sin maskine de to tal som ganget sammen giver resultatet 5.283.065.753.709.209, en beregning der med papir og blyant formentlig ville have taget adskillige år. Med introduktionen af computeren blev det selvfølgelig nemmere at faktorisere store heltal, men som vi allerede har nævnt har også computerne deres begrænsninger.

Kunne man blot bestemme om vilkårlige tal er primtal uden at være nødt til at faktorisere dem, så ville det først for alvor være smart. Et af de første forsøg med at opskrive en liste af samtlige primtal på snedig vis uden brug af faktorisering blev gjort allerede for over totusinde år siden, den såkaldte *Eratostenes' si*. Eratostenes (271-194 f.v.t.) var bibliotekar i Alexandrias bibliotek og havde altså blandt andet primtal som sin hobby. Eratostenes' si

er faktisk den mest effektive måde at konstruere en liste over samtlige primtal op til sådan cirka 1 million eller 10. Sien fungerer som følger: Først opskrives alle tal op til et eller andet n. Derefter stryges hvert tal i 2-tabellen på nær 2. Så stryges hvert tal i 3-tabellen på nær tre. 4 er væk, da 4-tabellen er en delmængde af 2-tabellen. Hvert tal i 5-tabellen på nær 5 stryges dernæst. 6 er væk, da 6-tabellen er en delmængde af 3-tabellen. Så stryges tallene i 7-tabellen på nær 7, og så videre. Tilbage har man en liste af primtal op til n. Processen afslører tilmed mindst én faktor af de sammensatte tal (hvordan?). Des højere tallene bliver des mindre effektiv begynder metoden dog fra et datalogisk synspunkt at være.

Som vi så beskæftigede Fermat sig også med om tal er primtal eller ej, og faktisk er hans lille sætning et af de mere vigtige værktøjer til sådanne bestemmelser – og det også uden at basere sig på faktoriseringer. Som set i afsnit 3.3 siger Fermats lille sætning, at hvis k er et primtal og n er et vilkårligt heltal, så er $n^k - n$ et multiplum af k. En anden formulering af denne sætning siger, at *hvis $n^k - n$ ikke et multiplum af k, så er k et sammensat tal*. Eksempelvis hvis $k = 9$ og $n = 2$ er udtrykket $2^9 - 2$ lig 510 som modulo 9 giver et resultat forskelligt fra nul, nemlig 6. Altså er det med den lille sætning muligt, omend måske lidt ad omveje, at konkludere at 9 ikke er et primtal. En test af om et tal er primtal eller ej ved brug af den lille sætning kaldes for *Fermats test*. Det her givne eksempel med 9 er selvfølgelig ret så simpelt, men det giver alligevel en ide om, hvordan man ved hjælp af Fermats lille sætning er i stand til at teste, hvorvidt enorme heltal er primtal eller ej. (For andre mere regnetunge eksempler se opgave 51.) Imidlertid løser Fermats test ikke fuldstændig problemet med at teste for primtal; hvis for et tal n tallet $n^k - n$ giver en rest forskellig fra nul modulo k er k bestemt et sammensat tal, men hvis nu vi får resten nul, kan k så stadig være et sammensat tal? Eller sagt på en anden måde, hvis Fermats test giver rest nul kan vi så være sikre på, at k er et primtal? Faktisk antyder en række eksempler dette: $2^2 - 2$ er et multiplum af 2, $2^3 - 2$ er et multiplum af 3, $2^5 - 2$ er et multiplum af 5, $2^7 - 2$ er et multiplum af 7, og tallene 2, 3, 5 og 7 er alle primtal. Kineserne opdagede for godt 2500 år siden dette mønster og mente derfor, at hvis $2^k - 2$ var et multiplum af k måtte k være et primtal. Dette 'resultat' er fremlagt i værket *I Ching* som Leibniz studerede i forbindelse med sine arbejde med binære tal, og derfor troede også han, at resultatet var sandt. I 1819 fandt den franske matematiker Pierre Frédéric Sarrus (1798-1861) imidlertid et modeksempel. Sarrus observerede, at $2^{341} - 2$ er et multiplum af 341 til trods for at 341 er et sammensat tal, idet $341 = 11 \cdot 31$. Sådanne sammensatte tal som formår at skjule sig for Fermats test kaldes for *pseudoprimtal*. Hvis n, som i tilfældet med Sarrus' modeksempel, er lig 2 taler man om *pseudoprimtal i talbase 2*. Det er blevet regnet ud, at antallet af pseudoprimtal i talbase 2 mindre end tallet 20 milliarder kun er 19.865. Det vil sige, at hvis Fermats test blev udført i talbase 2 for alle tal mindre end 20 milliarder ville der kun være en fejlmargin på 1 milliontedel. Det er ikke særlig meget, men hvis man ønsker at kunne teste om samtlige tal er primtal eller ej er det naturligvis ikke godt nok. Begrebet pseudoprimtal i talbase 2 kan

selvfølgelig generaliseres til *pseudoprimtal i talbase* n. Tallet $3^{91} - 3$ er et multiplum af det sammensatte tal 91 og er således et pseudoprimtal i talbase 3. Det viser sig, at der for hver talbase n findes uendeligt mange pseudoprimtal. Og ikke nok med det, der findes sammensatte tal som er pseudoprimtal til enhver talbase n, sådanne tal kaldes *Carmichael-tal* efter den amerikanske matematiker Robert Daniel Carmichael (1879-1967) som beskrev sådanne i 1919. Eksempler på Carmichael-tal er $561 = 3 \cdot 11 \cdot 17$ og $1729 = 7 \cdot 13 \cdot 19$. Eksistensen af Carmichael-tal spolerer alt håb for Fermats test som en måde at separere alle primtal fra sammensatte tal på.

Som nævnt i afsnit 2.4 omhandler et interessant spørgsmål, hvordan primtallene fordeler sig jo længere og længere man bevæger sig ud af tallinien. Udover at svaret på dette spørgsmål ville give en dyb indsigt i primtallenes natur, så ville det også give en måde at identificere nye kandidater til primtal på. Imidlertid er spørgsmålet i høj grad stadig ubesvaret. En af de ting man dog ved er, at der bliver længere og længere imellem primtallene når man bevæger sig ud af tallinien. Dette faktum kan nemt illustreres, idet man kan vise, at der findes vilkårligt lange stræk bestående udelukkende af sammensatte tal: For et vilkårligt naturligt tal n betragter vi $n! + k$ for $k = 2, 3, \ldots, n$. Der gælder, at

$$n! + k = 1 \cdot 2 \cdots k \cdots n + k = k(1 \cdot 2 \cdots (k-1)(k+1) \cdots n + 1),$$

eller sagt med andre ord, at k er en faktor i $n! + k$. Listen

$$n! + 2,\ n! + 3,\ \ldots,\ n! + n$$

udgør således et stræk af $n - 1$ på hinanden følgende sammensatte tal. Primtallenes fordeling ud af tallinien er et spørgsmål som har optaget adskillige matematikere igennem tiden og har således været årsag til diverse gæt, formodninger og hypoteser. En af de mere sejlivede af disse er *Riemann-hypotesen*.

Georg Friderich Bernhard Riemann (1826-1866) var ligesom Gauss et vidunderbarn. Som ganske ung tyggede han sig eksempelvis igennem Legendres 900 siders værk om talteori på blot seks dage. Riemann indleverede rent faktisk sin doktorafhandling til netop Gauss, omend denne dog ikke omhandlede talteori, men derimod geometri. Riemanns eneste arbejde om talteori, *Über die Anzahl der Primzahlen unter einer gegebenen Größe*, fremlagde han for akademiet i Berlin i 1859. Matematikken i Riemanns hypotese er for alt kompliceret til at gå i dybden med her, så vi skal nøjes med at give en forklaring i ord. Faktisk forholder det sig sådan, at løsningerne på flere af talteoriens mere genstridige problemer, eller forsøgene på at løse disse, ofte involverer ganske avanceret matematik som ikke selv hører under talteori. Udover Riemanns hypotese er Wiles' løsning af Fermats sidste sætning også et eksempel herpå. Før vi kan kan forstå vigtigheden af Riemanns hypotese, må vi først have forklaret en anden sætning, nemlig *primtalssætningen*. Primtalssætningen udtaler sig om antallet af primtal mindre end eller lig et naturligt tal n, et antal der betegnes $\pi(n)$ (det græske bogstav pi). Sætningen giver et estimat

for funktionen $\pi(n)$ når man lader n vokse. En af de første som opstillede et estimat for $\pi(n)$ var Gauss, som gjorde dette i 1792 i en alder af kun femten år. I og med at primtalssætningen kun er et estimat er den genstand for en vis usikkerhed, eller sagt med andre ord så har den en fejlmargin, og det er her Riemann-hypotesen kommer ind i billedet. Størrelsen af fejlleddet i primtalssætningen afhænger nemlig af, hvorvidt Riemann-hypotesen er sand eller ej. I 1901 blev det vist, at hvis Riemann-hypotesen er sand, så kan man beregne dette fejlled præcist. Man har da at $\pi(n)$ er lig Gauss' estimat plus dette præcist angivne fejlled. En sådan præcis angivelse af antallet af primtal mindre end et tal n kan for eksempel være nyttig hvis man vil være sikker på, at man har fundet samtlige primtal mindre end n.

Riemann-hypotesen er i dag et af de matematiske problemer der ligefrem er udlovet en dusør på, idet hypotesen indgår som et af de syv *Millennium Prize Problems*.[2] Be- eller afviser man således hypotesen vil man få én million dollars udbetalt af Clay Mathematics Institute i Cambridge, Massachusetts. Pengepræmier i forbindelse med løsningen af 'genstridige' matematiske problemer er efterhånden ikke nogen ualmindelighed og inden for talteorien findes der flere af slagsen. Eksempelvis modtog Wiles Wolfskehl-prisen for beviset af Fermats sidste sætning, en pris som oprindeligt var på et to-cifret millionbeløb, men som inflationen i Tyskland efter første verdenskrig havde reduceret til cirka 50.000 dollars. Set fra vores perspektiv kan Riemann-hypotesen, i fald den er sand, også gå hen og have en betydning for RSA-kryptering, hvilket vi skal berøre igen i næste kapitel. Men RSA-kryptering er langt fra det eneste som sandheden af formodningen vil have en betydning for. Rent faktisk har en hel del matematikere set sig nødsaget til at basere deres arbejde på en antagelse om at hypotesen er sand, for at nå deres egne mål. Dette er også grunden til at der fortrinsvist tales om en hypotese frem for en formodning. Betegnelsen en *hypotese* antyder i højre grad, at der er tale om en nødvendig antagelse som matematikere foretager for at opstille teorier. En *formodning* derimod repræsenterer en forudsigelse af, hvordan matematikere tror deres verden opfører sig. I tilfælde af at Riemann-hypotesen en dag vises sand vil sandheden af adskillige andre matematiske resultater således følge med i købet.

Et eksempel på en formodning inden for talteori er netop den tidligere nævnte *Goldbachs formodning*. Denne blev i sin nuværende form fremsat af Euler efter han havde modtaget et brev fra Goldbach i 1742. Goldbach beskrev i brevet nogle af hans overvejelser angående, hvorledes heltal kan udtrykkes som summer af primtal. Specielt påpegede han, at han mente, at ethvert heltal (større end 2) kan udtrykkes som summen af tre primtal. På dette tidspunkt var det stadig ikke helt afklaret, om det var smartest at regne 1 som et primtal eller ikke, og Goldbach regnede således 1 for værende primtal. Euler var dog ikke sen til at indse, at man kunne opstille den stærkere formodning, at ethvert lige tal (større end 2) kan skrives som summen af to primtal (når man ikke regner 1 for at være et primtal). Og det er denne

[2] En beskrivelse af problemerne kan findes på følgende hjemmeside: `http://www.claymath.org/millennium/`

formodning der i dag er kendt som Goldbachs formodning. Lad os se, hvordan det ser ud:

$$\begin{aligned}
4 &= 2+2 \\
6 &= 3+3 \\
8 &= 3+5 \\
10 &= 3+7 = 5+5 \\
12 &= 5+7 \\
14 &= 3+11 = 7+7 \\
16 &= 3+13 = 5+11 \\
18 &= 5+13 = 7+11 \\
20 &= 3+17 = 7+13 \\
22 &= 3+19 = 5+17 = 11+11 \\
&\vdots
\end{aligned}$$

Der gælder selvfølgelig, at jo større de lige tal bliver jo flere forskellige måder er der at udtrykke dem som summen af to primtal på. Goldbachs formodning blev i 1998 efterprøvet for tal op til $4 \cdot 10^{14}$, og den holdt. Det generelle bevis for den er dog stadig ikke fundet. Også beviset for Goldbachs formodning var der i en periode udlovet en pengepræmie for. Forlaget Faber & Faber udlovede i forbindelse med lanceringen af Apolostoldos Doxiadis' roman *Uncle Petros and Goldbach's Conjecture* én million engelske pund til den der beviste formodningen.[3] Tilbuddet gjaldt dog kun i en to-årig periode begyndende den 20. marts 2000 og endnu mere mærkeligt var det, at tilbuddet kun gjaldt personer som var lovlige statsborgere i enten Storbritannien eller USA samt over 18 år gamle. Hverken Goldbach eller Euler ville således have været i stand til at indkassere præmien havde de haft et bevis (og været i live).

Udover de ovenstående mere seriøse uløste aspekter af talteorien findes der et hav af diverse kuriøsiteter om primtal. Et af disse omhandler de såkaldte *tvillingeprimtal*. Tvillingeprimtal er to primtal som kommer lige efter hinanden,

$$3 \text{ \& } 5,\ 5 \text{ \& } 7,\ 11 \text{ \& } 13,\ 17 \text{ \& } 19,\ 29 \text{ \& } 31, \ldots$$

Det forekommer klart, at des længere man bevæger sig ud af tallinien des længere vil der være imellem tvillingerne. Ikke desto mindre siger *tvillingeprimtalformodningen*, at der findes uendeligt mange tvillingeprimtal. De største kendte tvillinger er $33218925 \cdot 2^{169690} \pm 1$ som hver har 51.090 cifre og blev fundet i 2002. Tvillingeprimtal er faktisk nogle af de mere seriøse af primtalskuriøsiteterne. Eksempler på de useriøse kuriøsiteter er de såkaldte *palindromprimtal*, hvilket vil sige at tallene kan læses fra begge sider, som eksempelvis primtallet 12421. Af den helt useriøse slags er *James Bondprimtallene*, som er... ja, primtal som ender på 007. De tre første af disse er 4007, 6007 og 9007.

[3] Bogen er i Danmark udkommet på Gyldendal under titlen *Onkel Petros og Goldbachs formodning*.

Som det fremgår af ovenstående er talteori blevet et mere og mere anerkendt og udbredt forskningsområde blandt matematikere, først i løbet af det 19. århundrede, ikke mindst med Gauss, og siden op igennem det 20. århundrede. En af de vigtigste matematikere i det 20. århundrede hvad angår talteori er den britiske matematiker G. H. Hardy (1877-1947). Hardy var en fortaler for, hvad man kan kalde *ren* matematik i modsætning til *anvendt* matematik. For eksempel sagde han, at han var »interesseret i matematik alene som en kreativ kunstform« og udtrykte sin tilfredshed med, at intet af det matematik han havde bedrevet havde nogen form for praktisk anvendelse. Hardys utilfredshed med anvendt videnskab skyldtes det faktum, at han nåede at opleve to verdenskrige, hvor han var vidne til, hvad man med rette kan kalde misbrug af naturvidenskaberne. Hardy udtrykte sig på følgende ironiske vis: »En videnskab siges at være nyttig, hvis dens udvikling forstærker ulighed blandt mennesker eller mere direkte medvirker til udslettelsen af menneskeliv« og tilføjede efter sigende hertil, at studiet af primtal ikke gjorde nogen af delene (Hardy, 1915 i Wells (2005, side 135)). Lige så berømt som Hardy er for sine bedrifter inden for matematik, lige så berømt er han også for sine udtalelser *om* matematik og matematikere og ikke mindst forholdene mellem disse og politik. På et postkort til en bekendt skulle Hardy engang have nedfældet seks nytårsønsker. Et af disse ønsker var at få lejlighed til at myrde Mussolini, et andet at score 211 point i fjerde inning af en afgørende cricketkamp (Hardy var en lidenskabelig og talentfuld kricketspiller), men det første ønske var at bevise Riemann-hypotesen. Et af Hardys mest berømte skrifter om matematik og det at bedrive denne videnskab er hans *A Mathematician's Apology* fra 1940, som vi skal se nærmere på som del af den afsluttende essay-opgave (se opgave 74).

Hardy betragtede altså talteori og i særdeleshed studiet af primtal som en af de reneste former for matematik, idet disse ingen praktiske anvendelser

G. F. Bernhard Riemann (1826-1866)

G. H. Hardy (1877-1947)

havde og derfor ikke kunne være genstande for misbrug i politisk øjemed. Hvis Hardy havde levet tredive år længere ville han nok være blevet skuffet. Talteori fandt sine første praktiske anvendelser i forbindelse med kodningsteori og studiet af fejlkorrigerende koder i 1950'erne og 1960'erne. Og i 1970'erne fandt primtalsteori sin praktiske anvendelse i asymmetrisk kryptografi, eller nærmere bestemt RSA-kryptering. På dette tidspunkt var den elementære talteori over 2000 år gammel og det nyeste resultat brugt i RSA, Eulers sætning, lidt over 200 år gammelt. Det interessante spørgsmål i denne forbindelse er dog, hvorfor der skulle gå mere end 200 år førend man fandt på at anvende disse resultater i kryptografi, når nu ideen om kryptering i sig selv er lige så gammel som den elementære talteori. En del af svaret på dette spørgsmål har vi allerede fået præsenteret i kapitel 1. I næste kapitel skal vi fortsætte behandlingen af såvel dette som andre relaterede spørgsmål.

3.6 Opgaver

Opgave 32
Forklar hvad der forstås ved begreberne: Modulo, kongruens, lineær kongruens, invers af heltallet a modulo m, Eulers ϕ-funktion, pseudoprimtal, pseudoprimtal i talbase n, Carmichael-tal, tvillingeprimtal.

Opgave 33
Hvad siger følgende sætninger: Den kinesiske restsætning, Fermats lille sætning og Eulers sætning.

Opgave 34
Forklar hvad der forstås ved et konstruktivt bevis og ved et ikke-konstruktivt bevis.

Opgave 35
Et værtshusspil, som spilles om øl af to personer, gå ud på at den ene spiller begynder med at sige 1 eller 2. Den anden spiller lægger da enten tallet 1 eller tallet 2 til det som den første spiller sagde og fremsiger resultatet. Første spiller lægger nu 1 eller 2 til det som anden spiller sagde, og sådan fortsættes spillet indtil man når 30. Den der ved at lægge 1 eller 2 til det der sidst er sagt og derved får resultatet 30 er vinderen af spillet (og vinder en øl fra den anden).

a. Spil et par omgange af spillet med din sidemand og forsøg derved at finde ud af hvilken strategi man skal lægge for at vinde spillet. (Altså hvilke tal man skal ramme for at være sikker på at sige 30.)
b. Spillet spilles nu igen men denne gang med den ændring at der kun spilles til 20. Hvilke tal skal man nu ramme for at være sikker på at vinde?
c. Ved hjælp af modulo-regning ønskes ovenstående strategier nu generaliseret til et spil, hvor man spiller til et vilkårligt men fastlagt naturligt tal T, og hvor man skiftes til at lægge de ligeledes vilkårlige men fastlagte naturlige tal n og m til. (Hvis man kan løse denne opgave skulle der være basis for at vinde endnu flere øl på værtshusene.)

Opgave 36
Undersøg med udgangspunkt i definition 3.1 hvilke af følgende udsagn er sande henholdsvis falske:
a. $10 \equiv 1 \pmod 3$.
b. $39 \equiv 4 \pmod 5$.
c. $131 \equiv 1 \pmod{13}$.
d. $2093 \equiv 5 \pmod{19}$.
e. $10 \equiv 4 \pmod 3$.

Opgave 37
Undersøg med udgangspunkt i sætning 3.5 hvilke af følgende udsagn er sande henholdsvis falske:
a. $111 \equiv 3 \pmod{11}$.
b. $111 \equiv 12 \pmod{11}$.
c. $349 \equiv 9 \pmod{17}$.
d. $3017 \equiv 3 \pmod{15}$.
e. $444 \equiv 0 \pmod 6$.

Opgave 38
For hver af de sande udsagn, $a \equiv b \pmod m$, i opgaverne 36 og 37 angiv da k således at $a = b + km$.

Opgave 39
Bøger identificeres ved et *International Standard Book Number* (ISBN), hvilket er en 10-cifret kode $x_1x_2 \ldots x_{10}$, som tildeles af forlaget. De 10 cifre består af blokke som identificerer sprog, forlag, det af forlaget givne nummer til bogen og endelig ét kontrolciffer, som er enten et ciffer eller et X (brugt til at repræsentere 10). Kontrolcifret vælges således, at

$$1x_1 + 2x_2 + 3x_3 + \ldots + 10x_{10} \equiv 0 \pmod{11}.$$

a. De første ni cifre i Simon Singhs *The Code Book* er 185702889-, hvad er kontrolcifret?
b. Hvis ISBN for en bog er 020157Q98-1, hvad er da værdien af Q?
c. Kontroller om kontrolcifret i ISBN, 052142706-1, for 1967-udgaven af G.H. Hardys *A Mathematician's Apology* er korrekt.

Opgave 40
Vis, at:
a. 15 er en invers af 7 modulo 2.
b. 937 er en invers af 13 modulo 2436.

Opgave 41
Find en invers af:
a. 4 modulo 9.
b. 2 modulo 17.
c. 19 modulo 141.
d. 144 modulo 233.

Opgave 42
Løs følgende lineære kongruenser:
a. $4x \equiv 5 \pmod 9$.
b. $2x \equiv 7 \pmod{17}$.

Opgave 43
Bestem løsningerne til følgende system af kongruenser: $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 3 \pmod 5$.

Opgave 44
Bestem løsningerne til følgende system af kongruenser: $x \equiv 7 \pmod 9$, $x \equiv 0 \pmod 4$, $x \equiv 2 \pmod 7$.

Opgave 45 (Historisk opgave)
Figur 3.2 viser den kinesiske restsætning som præsenteret af Sun Zi og giver samtidig en oversættelse til dansk. Med udgangspunkt i Sun Zis formulering af sætningen ønskes følgende gjort:
a. Udfør først det af Sun Zi givne regnestykke ved hjælp af metoden givet af Sun Zi.
b. Udfør dernæst det samme regnestykke ved hjælp af den moderne formulering af den kinesiske restsætning, sætning 3.18.
c. Synes du, at Sun Zi giver et bevis for den kinesiske restsætning? Argumenter for dit svar.

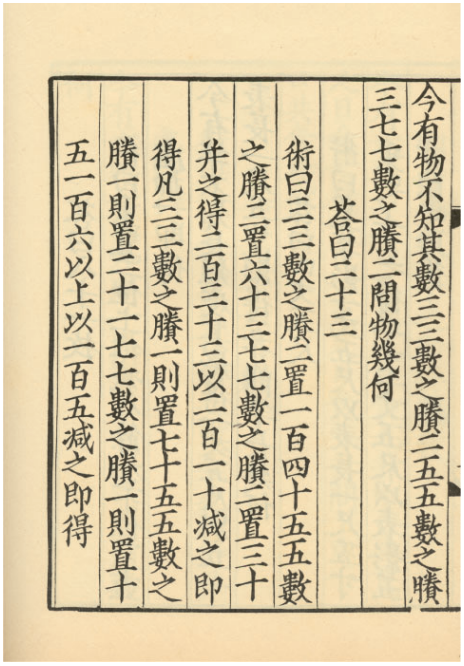
Opgave 46 (Historisk opgave)
Fermat omtaler i sit brev til Frenicle af 10. oktober, 1640 hvad der i dag er kendt som 'Fermats lille sætning':

> Ethvert primtal er altid en faktor i en af potenserne af en vilkårlig progression minus 1, og eksponenten af denne potens er en faktor i primtallet minus 1. Efter man har fundet den første potens som opfylder propositionen, opfylder alle de potenser af hvilke eksponenterne er multipla af eksponenten af den første potens også propositionen.
> *Eksempel:* Lad den givne progression være:

1	2	3	4	5	6	
3	9	27	81	243	729	etc.

med dens eksponenter skrevet øverst.
Tag nu for eksempel primtallet 13. Det er en faktor i den tredje potens minus 1, af hvilken 3 er eksponenten og en faktor i 12, hvilket er én mindre end tallet 13, og fordi eksponenten af 729, som er 6, er et multiplum af den første eksponent, som er 3, følger det at 13 også er en faktor i denne potens 729 minus 1. (Struik; 1969, side 28, oversat fra engelsk)

a. Forklar med dine egne ord hvad det er Fermat siger i ovenstående citat, herunder hvad han forstår ved 'eksponent', 'potens' og 'progression'.
b. Opskriv de næste tre led i den progression som Fermat selv giver som eksempel.
c. Oversæt Fermats eksempel med primtallet 13 til moderne notation anvendende kongruenser.
d. Hvad sker der hvis man indsætter andre primtal end 13 i den givne progression? Gælder propositionen (Fermats lille sætning) da stadig?


今有物不知其數三三數之賸二五五數之賸
三七七數之賸二問物幾何
答曰二十三
術曰三三數之賸二置一百四十五五數
之賸三置六十三七七數之賸二置三十
并之得二百三十三以二百一十減之即
得凡三三數之賸一則置七十五五數之
賸一則置二十一七七數之賸一則置十
五一百六以上以一百五減之即得

Nu er der et ukendt antal af ting. Hvis vi tæller i treere, er der en rest 2; hvis vi tæller i femmere, er der en rest 3; hvis vi tæller i syvere, er der en rest 2. Find antallet af ting. Svar: 23.
Metode: Hvis vi tæller i treere og der er en rest 2, nedskriv 140. Hvis vi tæller i femmere og der er en rest 3, nedskriv 63. Hvis vi tæller i syvere og der er en rest 2, nedskriv 30. Læg dem sammen for at få 233 og træk 210 fra for at få svaret. Hvis vi tæller i treere og der er en rest 1, nedskriv 70. Hvis vi tæller i femmere og der er en rest 1, nedskriv 21. Hvis vi tæller i syvere og der er en rest 1, nedskriv 15. Når [et tal] overstiger 106 fås resultatet ved at fratrække 105. (Yong & Se; 1992, side 219-220, oversat fra engelsk)

Figur 3.2 Den kinesiske restsætning som fremlagt af Sun Zi i *Sunzi suanjing*.

Opgave 47
Beregn for følgende værdier af m Eulers ϕ-funktion, $\phi(m)$:
a. $m = 4$.
b. $m = 10$.
c. $m = 13$.
d. $m = 12$.
e. $m = 30$.

Opgave 48
Undersøg hvilke af de i opgave 47 givne m-værdier der opfylder betingelserne for Eulers sætning, hvis $n = 3$. For de som gør, udregn da $n^{\phi(m)}$ og godtgør at dette tal er kongruent med 1 modulo m.

Opgave 49
Vis, at $\phi(p^k) = p^k(1 - 1/p)$ når p er et primtal og $k > 0$ er et heltal.

Opgave 50
Opskrive tallene fra 1-100 i et 10×10 skema og udsæt derefter disse for Eratostenes' si. Hvilke mønstre eller systemer kan du se, når Eratostenes' si opererer på et skema som dette?

Opgave 51
Forklar hvordan Fermats lille sætning kan bruges til at teste om et tal er et primtal – den såkaldte Fermats test – og løs derefter følgende opgaver:
a. Ved hjælp af Fermats test med $n = 2$ bestem da hvilke af fire følgende tal som man med sikkerhed kan konkludere er sammensatte tal: 103, 117, 341, 561. (Vink: Computerens lommeregner kan med fordel bruges til dette.)
b. Udsæt nu de tal, af de fire ovenfor, som vi ikke med sikkerhed kan vide om er sammensatte tal for Fermats test med $n = 3$. Tal som kan konkluderes sammensatte nu, men ikke blev det før, er såkaldte pseudoprimtal. Hvilke tal er herefter tilbage?
c. Kan man sige noget om de tilbageværende tal?

Opgave 52
Forklar hvorfor det netop er Carmichael-tallene og ikke pseudoprimtallene i sig selv der spolerer alt håb for Fermats test.

Opgave 53
Forklar hvad Wilsons sætning siger. Forklar dernæst hvordan Wilsons sætning kan bruges til at teste om et tal er et primtal og diskuter, hvorvidt Wilsons sætning synes hensigtsmæssig til brug i en sådan test.

Opgave 54
Opskriv en liste af 20 på hinanden følgende sammensatte tal.

Opgave 55 (Historisk opgave)
Som beskrevet i afsnit 3.5 beretter Goldbach i 1742 om sin formodning til Euler. Goldbach skriver følgende:

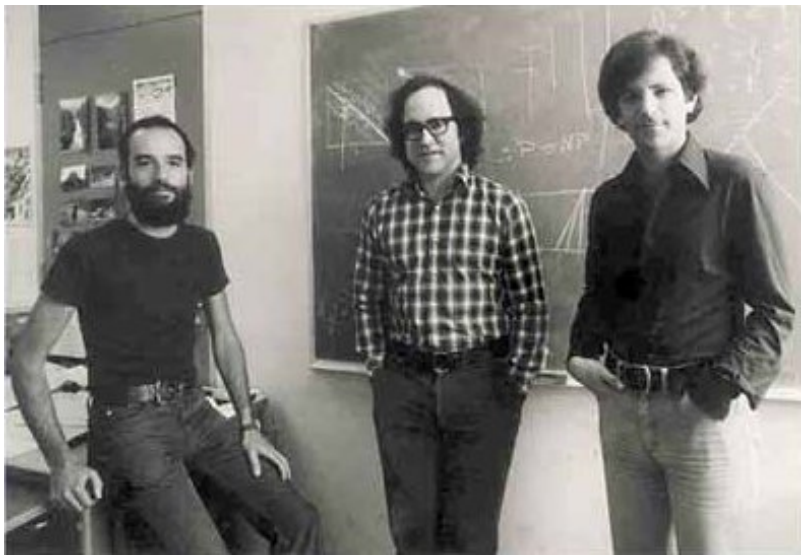
> Jeg skal vove en formodning: at ethvert tal som er komponeret af to primtal er en sammenlægning af så mange tal som vi ønsker (inklusive enhed), til kombinationen af samtlige enheder [er nået]. [Goldbach tilføjer i marginen:] Efter at have genlæst dette finder jeg, at formodningen kan demonstreres med fuld stringens for tilfældet $n + 1$, hvis den er opfyldt i tilfældet for n og hvis $n + 1$ kan deles op i to primtal. Demonstrationen er ganske let. I alle tilfælde lader det til, at ethvert heltal større end 2 er en sammenlægning af tre primtal. (Struik; 1969, side 47, oversat fra engelsk)

Det der i dag omtales som 'Goldbachs oprindelige formodning', inden Euler ændrede denne til den nuværende Goldbachs formodning (se afsnit 3.5), udgøres af den sidste sætning i citatet: »... ethvert heltal større end 2 er en sammenlægning af tre primtal.«

a. Forklar, hvad Goldbach mener med 'komponeret'.
b. Hvad forudsætter Goldbach implicit når han taler om 'kombinationen af samtlige enheder'?
c. For heltallene 1 op til og med 12 opskriv da for hvert tal samtlige af de kombinationer Goldbach omtaler.
d. Identificer i disse kombinationer de sammenlægninger som opfylder henholdsvis 'Goldbachs oprindelige formodning' og Eulers strengere 'Goldbachs formodning'.

4 RSA-algoritmen

Diffie og Hellmans artikel indeholdende ideen om offentlig-nøgle kryptering og brugen af en envejsfunktion blev genstand for stor interesse mange steder efter udgivelsen i 1976, men den blev kun genstand for realisering ét sted. Dette sted var på 8. sal af MITs institut for datalogi. Her sad tre unge forskere som tilsammen skulle komme til at udgøre et frugtbart team i realiseringen af ideen: Ronald Rivest, Adi Shamir og Leonard Adleman. Rivest var datalog med en bemærkelsesværdig evne til at absorbere nye ideer og anvende dem i utænkelige sammenhænge. Tilmed holdt han sig altid orienteret i de nyeste videnskabelige artikler. Shamir var ligeledes datalog og besad en uvurderlig evne til at betragte et problem og derefter trænge igennem til dettes kerne. Rivest og Shamir var begge optaget af kryptering og problemet med nøgle-distribution og kom derfor vældigt 'op at køre', da de blev bekendt med Diffies og Hellmans ideer. Adleman var matematiker (talteoretiker) og ikke hverken bekendt med eller i begyndelsen interesseret i kryptering og nøgle-distribueringsproblemet. Ikke desto mindre lykkedes det Rivest at overbevise Adleman om den rolle som matematik havde at spille i genereringen af



Adi Shamir (1952-), Ronald Rivest (1948-) og Leonard Adleman (1945-).

kandidater til envejsfunktioner opfyldende Diffie og Hellmans krav til et offentlig-nøgle system. Arbejdsproceduren imellem de tre blev således, at Rivest og Shamir i løbet af det næste år ville finde på et hav af énvejsfunktioner og Adlemans job var så at teste, hvorvidt disse opfyldte de givne krav.

Forfatteren Thomas A. Bass foretog i 1995 et interview med Adleman, hvori denne blandt andet fortalte om sit arbejde med kryptografi. Nedenstående er et uddrag af denne artikel.

> Efter at have afsluttet sin universitetsuddannelse i '76 [...] med en ph.d. i datalogi (hans afhandling omhandlede logik og talteori) [...] tog Adleman et undervisningsjob på MIT til US$13.000 om året. To andre unge forskere, Ron Rivest og Adi Shamir, sad i nabokontorerne og de blev alle snart gode venner. Men Rivest og Shamir havde en passion som i begyndelsen ikke blev delt af Adleman. En dag, det følgende år, bemærkede Adleman at Rivest havde et vildt udtryk i øjnene. Rivest tvang et udkast til en artikel af Whitfield Diffie og Martin Hellman ind i hænderne på Adleman og annoncerede deres teoretiske opdagelse af offentlig-nøgle kryptografi, en ny måde at indkode information på. Præcis hvordan resultatet kunne implementeres var stadig ikke kendt. Dette krævede noget ved navn en envejsfunktion – nem at beregne i en retning, men praktisk talt umulig at beregne i den modsatte retning. [...] Adlemans venner kunne ikke holde op med tale om envejsfunktioner og hemmelig kodebrydning og til sidst smittede deres entusiasme. Rivist og Shamir blev ved med at finde på ideer til, hvordan man kunne implementere et offentlig-nøgle kryptosystem, og Adleman, talteori-eksperten, blev anvist jobbet med at finde huller i disse. I løbet af de næste par måneder knækkede han 42 potentielle systemer. Nogle involverede ligninger som kunne løses i løbet af minutter, andre krævede en dag eller to med koncentreret tænkning. En nat [...] blev Adleman vækket ved et telefonopkald. Det var Rivest med offentlig-nøgle kryptosystem nummer 43. »Jeg vidste han havde fundet på det uovervindelige system«, siger Adleman, »man får en fornemmelse for disse ting, hvis man tænker længe nok på dem; min æstetiske dømmekraft fortalte mig, at han endelig havde gjort det.« Rivest blev oppe hele natten og skrev udkastet til en forskningsartikel, som han præsenterede for sine kollegaer den følgende morgen. Artiklen blev udgivet i *February 1978 Communications of the ACM* med fælles forfatterskab af Rivest, Shamir og Adleman, artiklens officielle titel var *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. (Metoden er i dag i vid udstrækning kendt under gruppens initialer *RSA*.) »Jeg troede, at dette ville være det ubetydeligste af alt mit arbejde«, siger Adleman. »Jeg var så naiv med hensyn til kryptografi og dets anvendelser.« Snart var de tre internationale skikkelser. Post fra hele verden begyndte at hobe sig op i Rivests kontor, inklusive mistænkeligt udseende breve fra forsvarsministeriet i Bulgarien. Så begyndte National Security

> Agency at kontakte dem. Adleman havde aldrig før hørt om NSA, statens hemmelige spion-apparatur (husk, at dette var i '70'erne); spioner ringede og sagde, at den amerikanske stat klassificerede kryptografi i samme kategori som våben og ammunition, og hvis de sendte deres artikel udenfor landets grænser ville de blive retsforfulgt for ulovlig våbenhandel. Men det var for sent! Ånden var allerede ude af flasken. Mod slutningen af '70'erne var kryptografikonferencer blomstret op over hele USA og Europa – kryptografi var blevet sin egen matematiske disciplin. »Lige siden vores artikel udkom, er det aldrig holdt op igen«, siger Adleman, »videnskabeligt, forretningsmæssigt, politisk.« (Bass; 1995, oversat fra engelsk)

Første gang eksistensen af Rivest, Shamir og Adlemans arbejde blev offentliggjort var i 1977, hvor det indgik i Martin Gardners sædvanlige indslag *Mathematical Games* i tidsskriftet *Scientific American*. Gardner præsenterede under overskriften »A New Kind of Cipher that Would take Millions of Years to Break« en kryptotekst og den tilhørende offentlige nøgle som havde været brugt til at kryptere den med, nemlig heltallet

$$\begin{aligned} n \;=\; & 114381625757888867669235779976146612010218 2 \\ & 967212423625625618429357069352457338978305 9 \\ & 712356395870505898907514759929002687954354 1, \end{aligned}$$

et tal på 129 cifre. Gardner udfordrede sine læsere til at primfaktorisere dette tal og derpå bryde koden. Måden hvorpå selve krypteringsalgoritmen (RSA) fungerede beskrev Gardner dog ikke i sin artikel, men henviste i stedet sine læsere til de tre MIT-forskere for en beskrivelse af dette. Rivest, Shamir og Adleman modtog over tretusinde breve fra læsere af Gardnes kolonne og det var blandt andet disse breve som hobede sig op på Rivests kontor. De tre forskere besvarede dog ikke brevene med det samme, idet de gerne ville have indsendt en ansøgning om patentrettighederne for deres algoritme først. Da dette var gjort blev der holdt en lille højtidelighed på MITs institut for datalogi, hvor Rivest, Shamir og Adleman sørgede for pizza og øl og de indbudte, lige fra professorer til studerende, puttede tekniske beskrivelser af RSA-algoritmen i konvolutter til læsere af *Scientific American*.

Inden vi skal se, hvad det var for en algoritme som læserne af Gardners kolonne modtog med posten, skal vi lige kaste endnu et blik på Cæsar-kryptering og i den forbindelse se, hvordan man kan formulere denne krypteringsprocedure i termer af modulo-regning. Ligeledes tjener dette gensyn til at minde os om, hvilke krav man bliver nødt til at stille til de anvendte kryptosystemer.

4.1 Et gensyn med Cæsar-kryptering

Ved hjælp af modulo-regning kan vi beskrive Cæsar-kryptering matematisk. Det første vi gør er at opstille et skema indeholdende de 29 bogstaver og bindestreg. Tabel 4.1 indeholder et sådant alfabet. Vi kan nu lade Cæsar-kryptering være repræsenteret af en funktion $\mathcal{C}$, som til ethvert

-	→	00	F	→	06	L	→	12	R	→	18	X	→	24
A	→	01	G	→	07	M	→	13	S	→	19	Y	→	25
B	→	02	H	→	08	N	→	14	T	→	20	Z	→	26
C	→	03	I	→	09	O	→	15	U	→	21	Æ	→	27
D	→	04	J	→	10	P	→	16	V	→	22	Ø	→	28
E	→	05	K	→	11	Q	→	17	W	→	23	Å	→	29

Tabel 4.1 Nummerering af de store bogstaver i alfabetet samt bindestreg.

ikke-negativt heltal x mindre end eller lig 29 knytter et andet heltal $\mathcal{C}(x) \in \{00, 01, \ldots, 29\}$ ved formlen

$$\mathcal{C}(x) = (x + 3) \text{ modulo } 30.$$

I den krypterede besked bliver bogstavet repræsenteret ved x altså udskriftet med bogstavet repræsenteret ved $x + 3$ modulo 30. Lad os se på eksemplet fra afsnit 1.1.

Eksempel 4.1
Vi har altså igen beskeden `TERNINGERNE ER KASTET`, men i stedet for som sidste gang at oversætte den direkte til bogstaverne tre pladser længere fremme i alfabetet oversætter vi den nu til tallene fra tabel 4.1. Vi får

$$20\,05\,18\,14\,09\,14\,07\,05\,18\,14\,05 \quad 05\,18 \quad 11\,01\,19\,20\,05\,20.$$

Man begynder dernæst fra en ende af:

$$\mathcal{C}(20) = (20 + 3) \text{ modulo } 30 = 23,$$

som svarer til `W` i tabellen. Man forsætter så således indtil man får den krypterede talbesked:

$$23\,08\,21\,17\,12\,17\,10\,08\,21\,17\,08 \quad 08\,21 \quad 14\,04\,22\,23\,08\,23,$$

som ved hjælp af tabellen oversættes til `WHUQLQJHUQH HU NDVWHW`.

Det smarte ved at lave Cæsar-kryptering om til matematik på denne måde bliver dog først rigtig tydeligt når man i forbindelse med enten kryptering eller dekryptering bliver nødt til at tælle forfra eller bagfra i alfabetet. Lad os antage at modtageren af Cæsars krypterede besked sender beskeden `ØV` tilbage. Oversættelsen ifølge tabellen bliver 28 22. Krypteringen af dette bliver:

$$\begin{aligned} \mathcal{C}(28) &= (28 + 3) \text{ modulo } 30 = 01, \\ \mathcal{C}(22) &= (22 + 3) \text{ modulo } 30 = 25, \end{aligned}$$

hvilket giver `AY`. ◇

Det at begynde at tælle henholdsvis forfra og bagfra i alfabetet er nu lige pludselig 'automatisk' indlejret i den matematiske formel som nu udgør Cærsars metode til kryptering. Brugen af modulo gør det også meget lettere at opskrive Cæsar-kryptering og dekryptering som en algoritme (se opgave 57).

Også RSA-kryptering gør brug af modulo-regning omend på en noget mere sofistikeret vis, idet brugen af kongruenser her er indlejret i de i kapitel 3 præsenterede talteoretiske resultater. Det som gør RSA til så stærkt et system, i forhold til for eksempel Cæsar-kryptering, er, at det udover at være resistent overfor simple angreb baseret på frekvensanalyse, bygger på et af matematikkens store (uløste) problemer; primfaktorisering af store heltal. Et problem hvor det er vældig nemt at gå den ene vej; at bestemme et stort heltal n ved at gange to eller flere store primtal sammen. Men hvor det for alle praktiske anvendelser er alt, alt for tidskrævende at gå den anden vej; at primfaktorisere n. Og netop denne matematiske envejsfunktion udgør grundstenen i Rivests, Shamirs og Adlemans kryptosystem. Lad os se hvordan.

4.2 RSA-kryptering og dekryptering

RSA-kryptosystemet består af såvel en procedure til (ind)kryptering af en meddelelse som en procedure til dekryptering af denne. Disse procedurer er fuldstændig fastlagt og der er derfor tale om en algoritme: *RSA-algoritmen.*

Ideen i RSA er at de to individer, Alice og Bob, der ønsker at udveksle en meddelelse på sikker vis begge er i besiddelse af en *offentlig* nøgle $K_{\mathcal{E}}$ til kryptering af denne (K står for 'key' og $\mathcal{E}$ for 'encryption'). Nøglen består af to positive heltal n og e, vi skriver $K_{\mathcal{E}} = (n, e)$. Her er

$$n = p \cdot q,$$

hvor p og q er store primtal (eksempelvis på 200 cifre hver) og heltallet e er valgt på en sådan måde, at

$$\text{sfd}(e, \phi(n)) = 1.$$

Ved hjælp af sætning 3.30 kan vi med det samme omskrive dette til

$$\text{sfd}(e, (p-1)(q-1)) = 1.$$

Primtallene p og q er hvad vi kan tænke på som 'tilfældige' primtal af en vis cifferlængde. Der findes metoder til at generere sådanne primtal, men det skal vi ikke komme nærmere ind på her. Pointen i RSA er at man ikke udsætter systemet for fare ved at gøre nøglen $K_{\mathcal{E}} = (n, e)$ offentlig. Som vi skal se nedenfor, skal man for at være i stand til dekryptere meddelelsen kende n's primfaktorisering pq, og som vi allerede har diskuteret i forbindelse med aritmetikkens fundamentalsætning er det at finde primfaktoriseringen for meget store heltal en så besværlig process, at det til dags dato i praksis ikke lader sig gøre. Hvorfor vi netop vælger heltallet e som vi gør vil fremgå senere.

Det første vi gør er at oversætte vores meddelelse i ord til et heltal mellem 0 og n. For nemheds skyld og for ikke at overstige n kan vi bryde en lang meddelelse op i mindre blokke. Disse kan så oversættes til heltal ved hjælp af det samme skema vi anvendte til Cæsar-kryptering i forrige afsnit, tabel 4.1. Vi kalder denne numeriske form, altså en sådan blok af vores meddelelse, for M. Krypteringen af M foregår ved at opløfte M i e og tage modulo n af resultatet. Ud af dette får vi et nyt heltal, kaldet C for kryptoteksten, som altså er resten af M^e ved division med n. Selve algoritmen for RSA-(ind)krypteringen, som vi vil kalde $\mathcal{E}$, kan altså opskrives som proceduren

$$C \equiv \mathcal{E}(M) \equiv M^e \pmod{n}. \tag{4.1}$$

Det vigtige at forstå i forbindelse med RSA-kryptosystemet er, at de to individer der ønsker at udveksle en meddelelse ikke benytter den samme offentlige nøgle $K_{\mathcal{E}}$ til kryptering. Når Alice sender en meddelelse til Bob benytter hun hans offentlige nøgle og når Bob sender en meddelelse til Alice benytter han hendes. Der er altså to offentlige nøgler i spil, hver med forskelligt n og e, og skulle vi bære os helt korrekt ad burde vi opskrive Alices nøgle som $K_{\mathcal{E}} = (n_A, e_A)$ og Bobs som $K_{\mathcal{E}} = (n_B, e_B)$. Udfra hver sin offentlige nøgle genererer Alice og Bob hver sin *private* nøgle $K_{\mathcal{D}}$ til dekryptering. Denne består af heltallet n samt et andet positivt heltal, d, som er valgt således, at det er en invers af e modulo $(p-1)(q-1)$. Med symboler skriver vi

$$ed \equiv 1 \pmod{(p-1)(q-1)}.$$

Bemærk, at da e er valgt således, at $\text{sfd}(e, (p-1)(q-1)) = 1$ ved vi fra sætning 3.13 at en sådan invers d eksisterer, og tilmed er entydig modulo $(p-1)(q-1)$. Dekrypteringsnøglerne for henholdsvis Alice og Bob er altså, $K_{\mathcal{D}} = (n_A, d_A)$ og $K_{\mathcal{D}} = (n_B, d_B)$. Dekrypteringen af den afsendte kryptotekst C sker nu ved hjælp af dekrypteringsalgoritmen, kaldet $\mathcal{D}$:

$$\mathcal{D}(C) \equiv C^d \pmod{n}. \tag{4.2}$$

Det spørgsmål der imidlertid står tilbage er om man nu også rent faktisk får meddelelsen M ud af at køre dekrypteringsalgoritmen på kryptoteksten C. Det kan man bevise matematisk at man gør og det er netop til dette formål, at vi får brug for de tre sætninger fra kapitel 3: Den kinesiske restsætning, Fermats lille sætning og Eulers sætning. Vi skal altså vise følgende sætning:

Sætning 4.2
Ved anvendelse af RSA-dekrypteringsalgoritmen, $\mathcal{D}(C)$, på kryptoteksten C fås den oprindeligt krypterede meddelelse M. Med symboler skriver vi

$$\mathcal{D}(C) \equiv M \pmod{n}.$$

Bevis
Vi skal vise, at C^d er kongruent med M modulo n. Vi omskriver først udtrykket for C^d på følgende vis:

$$\mathcal{D}(C) \equiv C^d \equiv (M^e)^d = M^{ed} \pmod{n}.$$

Vi skal herfra dele beviset op i to tilfælde: (1) hvor n og M er indbyrdes primiske og (2) hvor de ikke er.

(1) Hvis $\text{sfd}(n, M) = 1$ ved vi fra korollar 3.34 til Eulers sætning, at

$$M^{ed} \equiv M^{ed \pmod{\phi(n)}} \pmod{n}.$$

Da $\phi(n) = (p-1)(q-1)$ kan vi omskrive ovenstående til

$$M^{ed} \equiv M^{ed \pmod{(p-1)(q-1)}} \pmod{n}.$$

Da vi har at $ed \equiv 1 \pmod{(p-1)(q-1)}$, hvilket jo er det samme som ed modulo $(p-1)(q-1) = 1$, får vi i ovenstående

$$M^{ed} \equiv M^1 \equiv M \pmod{n}.$$

Da jo $C^d \equiv M^{ed} \pmod{n}$ følger, at

$$C^d \equiv M \pmod{n},$$

hvilket var det vi skulle vise.

(2) Hvis n og M ikke er indbyrdes primiske må de mindst have én faktor tilfælles. Da n har primfaktoriseringen pq må altså enten $p \mid M$ eller $q \mid M$. Vi lader nu q være den fælles faktor (hvis den fælles faktor er p kan vi blot omdøbe q og p og beviset vil være det samme). Hvis $q \mid M$, altså $M \equiv 0 \pmod{q}$, har vi naturligvis også, at $q \mid M^{ed}$, det vil sige $M^{ed} \equiv 0 \pmod{q}$. Af dette følger at $M^{ed} \equiv M \pmod{q}$, hvilket vi, da $M^{ed} = C^d$, kan skrive som

$$C^d \equiv M \pmod{q}.$$

Hvis vi nu blot kan vise, at C^d ligeledes er kongruent med M modulo p, så har vi ifølge den kinesiske restsætning, sætning 3.18, da jo p og q er primtal og derfor nødvendigvis indbyrdes primiske, at C^d er kongruent med M modulo pq, altså $C^d \equiv M \pmod{n}$. Vi skal derfor vise, at $C^d \equiv M \pmod{p}$, og kan vi det har vi også korrektheden af RSA i tilfældet $\text{sfd}(n, M) \neq 1$.

Vi bemærker, at hvis $ed \equiv 1 \pmod{(p-1)(q-1)}$, så findes der et heltal k således, at $ed = 1 + k(p-1)(q-1)$. Det følger heraf, at vi kan omskrive udtrykket for C^d på følgende vis:

$$\begin{aligned} C^d &\equiv M^{ed} \pmod{n} \\ &\equiv M^{1+k(p-1)(q-1)} \pmod{n} \\ &\equiv M \cdot M^{k(p-1)(q-1)} \pmod{n} \\ &\equiv M \cdot (M^{(p-1)})^{k(q-1)} \pmod{n} \end{aligned}$$

Da der for M i RSA er forudsat, at $0 < M < n$ har vi, at p og q ikke begge kan være faktorer i M, for i så fald ville M jo blive større end eller lig n. Altså har vi ifølge antagelsen om at $q \mid M$, at $p \nmid M$. Da p er et primtal følger heraf, at p og M er indbyrdes primiske. Men når $\text{sfd}(p, M) = 1$ har vi ifølge Fermats lille sætning, sætning 3.25, at

$$C^d \equiv M \cdot (M^{(p-1)})^{k(q-1)} \equiv M \cdot 1^{k(q-1)} \equiv M \pmod{p},$$

og dermed er vi færdige.

Vi har nu altså vist korrektheden af RSA-algoritmen i de to tilfælde hvor n og M henholdsvis er og ikke er indbyrdes primiske, det vil sige at der altid vil gælde, at

$$C^d \equiv M \pmod{n}.$$

□

Lad os nu se et eksempel på en kryptering og en dekryptering ved brug af RSA-algoritmen.

4.3 Et udførligt eksempel

Vi skal her illustrere hvad sætning 4.2 fortæller os ved at vise hvordan et RSA-kryptosystem fungerer. For nemhedens og illustrationens skyld vil vi operere med små tal. Igen kigger vi på den situation, hvor Alice vil sende en besked til Bob. Når Alice skal kryptere sin besked skal hun bruge nøglen, $K_{\mathcal{E}} = (n_B, e_B)$, som Bob har offentliggjort. Alice kender kun talværdierne i dette nøglepar, hun ved ikke hvordan Bob er kommet frem til dem og hvilke primtal der gemmer sig bag.

Selv om Alice ikke ved det kan vi jo selvfølgelig godt få det at vide. Bob har valgt de to primtal

$$p = 53 \quad \text{og} \quad q = 61,$$

hvilket har givet ham (og Alice) følgende heltal n:

$$n = p \cdot q = 53 \cdot 61 = 3233.$$

Dette er altså værdien n_B i den offentlige nøgle, den anden værdi, e_B, skal være et tal som er indbyrdes primisk med $\phi(n)$, hvilket jo er givet ved:

$$\phi(n) = (p-1)(q-1) = (53-1)(61-1) = 52 \cdot 60 = 3120.$$

Der skal altså bestemmes et tal e som opfylder, at

$$\text{sfd}(e, \phi(n)) = \text{sfd}(e, 3120) = 1$$

og det kan man gøre ved at prøve sig frem. Hvis man vælger et primtal kan man gøre dette lidt nemmere for sig selv, idet man da blot behøver at teste om primtallet er en divisor i $\phi(n)$ og er det ikke det vil kravet være

opfyldt (hvorfor?). 23 er et primtal og $23 \nmid 3120$, hvorfor Bob har valgt dette til sin e-værdi. Bobs offentlige nøgle til (ind)krypterering er altså

$$K_{\mathcal{E}} = (n_B, e_B) = (3233, 23).$$

(Bemærk, at e selvfølgelig også sagtens kunne have været et sammensat tal. I så tilfælde kunne man have benyttet Euklids algoritme til at undersøge om den største fællesdivisor var 1.)

For at teste om systemet fungerer har Alice valgt at sende Bob beskeden `RSA-KRYPTERING`. Det første der skal ske med denne besked er at den skal oversættes til et tal. Dette kan ske ved hjælp af tabel 4.1 fra afsnit 4.1:

$$1819010011182516200518091407.$$

Dette tal opdeles dernæst i blokke af størrelse mindre end n. Blokkene vælges så de består af fire cifre og vi får:

$$1819 \quad 0100 \quad 1118 \quad 2516 \quad 2005 \quad 1809 \quad 1407.$$

Hver af disse blokke, M, udgør nu en delmængde af den numeriske form af meddelelsen `RSA-KRYPTERING`. Krypteringen foregår dernæst ved hjælp af formlen

$$C \equiv \mathcal{E}(M) \equiv M^e \pmod{n}.$$

Den første blok vi skal udregne er altså

$$\mathcal{E}(1819) \equiv 1819^{23} \pmod{3233}.$$

Når man regner med så store tal som 1819^{23}, og endnu større tal hvilket vil forekomme når Bob skal dekryptere beskeden, kan det hænde at ens lommeregner giver en forkert rest, fordi den ikke regner med nok betydende cifre. Derfor er det smart at dele udregningen op i mindre stykker. Til dette kan man gøre brug af de velkendte potensregneregler, som i vores tilfælde her eksempelvis siger, at $1819^4 = (1819^2)^2$, $1819^8 = ((1819^2)^2)^2$, og så videre. Ideen er at man i sine udregninger løbende tager modulo, for således hele tiden at reducere størrelsen af de tal man regner med. Vi

(og Alice) har følgende:

$$\begin{aligned}
1819^1 \pmod{3233} &= 1819 \\
1819^2 \pmod{3233} &= 3308761 \pmod{3233} \\
&= 1402 \\
1819^4 \pmod{3233} &= 1402^2 \pmod{3233} \\
&= 1965604 \pmod{3233} \\
&= 3173 \\
1819^8 \pmod{3233} &= 3173^2 \pmod{3233} \\
&= 10067929 \pmod{3233} \\
&= 0367 \\
1819^{16} \pmod{3233} &= 0367^2 \pmod{3233} \\
&= 134689 \pmod{3233} \\
&= 2136.
\end{aligned}$$

Potensregnereglerne komme nu ind i billedet ved at man foretager følgende omskrivning:

$$1819^{23} = 1819^{16+4+2+1} = 1819^{16} \cdot 1819^4 \cdot 1819^2 \cdot 1819.$$

Fra udregningerne ovenfor kan der opskrives følgende:

$$\begin{aligned}
\mathcal{E}(1819) \equiv 1819^{23} \pmod{3233} &= 2136 \cdot 3173 \cdot 1402 \cdot 1819 \pmod{3233} \\
&= 17284309451664 \pmod{3233} \\
&= 0255.
\end{aligned}$$

Kryptoteksten C for den første blok bestående af fire cifre er således 0255. På lignende vis findes kryptoteksten for de resterende blokke til at være følgende:

$$\begin{aligned}
\mathcal{E}(0100) &\equiv 0100^{23} \pmod{3233} = 1391 \\
\mathcal{E}(1118) &\equiv 1118^{23} \pmod{3233} = 1046 \\
\mathcal{E}(2516) &\equiv 2516^{23} \pmod{3233} = 1733 \\
\mathcal{E}(2005) &\equiv 2005^{23} \pmod{3233} = 1745 \\
\mathcal{E}(1809) &\equiv 1809^{23} \pmod{3233} = 1554 \\
\mathcal{E}(1407) &\equiv 1407^{23} \pmod{3233} = 1808
\end{aligned}$$

Når samtlige blokke sættes sammen fås således den samlede kryptotekst

$$025513911046173317451554 1808.$$

Alice sender nu denne kryptotekst til Bob. Det første Bob gør er at bryde den op i blokke på fire cifre:

$$0255 \quad 1391 \quad 1046 \quad 1733 \quad 1745 \quad 1554 \quad 1808.$$

Bob skal nu bruge sin egen private nøgle, $K_{\mathcal{D}} = (n_B, d_B)$, til at dekryptere beskeden med. n_B er selvfølgelig den samme værdi som i den offentlige nøgle, men lad os se hvordan Bob har bestemt værdien d.

Den private nøgle d skal vælges således, at den er en invers af $e = 23$ modulo $\phi(n) = 3120$. Vi ved fra tidligere (jævnfør eksempel 3.14), at vi kan bestemme inverse ved at gå 'baglæns' gennem Euklids algoritme, og derefter udtrykke den største fællesdivisor som en sum af de to heltal, i tilfældet her

$$1 = s \cdot e + t \cdot \phi(n),$$

hvor s'et her er identisk med vores d-værdi. Men før vi kan gå baglæns i Euklids algoritme må vi nødvendigvis gå forlæns først. Selvfølgelig ved vi allerede at $\text{sfd}(e, \phi(n)) = 1$, for sådan er den jo valgt, men det hjælper os ikke, da det er mellemregningerne vi har brug for. Altså kører vi Euklids algoritme igennem for $\text{sfd}(23, 3120)$:

$$\begin{aligned} 3120 &= 23 \cdot 135 + 15 \\ 23 &= 15 \cdot 1 + 8 \\ 15 &= 8 \cdot 1 + 7 \\ 8 &= 7 \cdot 1 + 1 \\ 7 &= 1 \cdot 7 + 0 \end{aligned}$$

Vi finder som ventet $\text{sfd}(23, 3120) = 1$ og kan nu gå baglæns:

$$\begin{aligned} 1 &= 8 - 7 \cdot 1 = 1 \cdot 8 + (-1) \cdot 7 \\ &= 1 \cdot 8 + (-1) \cdot (15 - 8 \cdot 1) = (-1) \cdot 15 + 2 \cdot 8 \\ &= (-1) \cdot 15 + 2 \cdot (23 - 15 \cdot 1) = 2 \cdot 23 + (-3) \cdot 15 \\ &= 2 \cdot 23 + (-3) \cdot (3120 - 23 \cdot 135) = (-3) \cdot 3120 + 407 \cdot 23. \end{aligned}$$

Vi får således, at

$$1 = -3 \cdot \phi(n) + 407 \cdot e,$$

hvilket betyder at $d = 407$.

Altså har Bob den private dekrypteringsnøgle givet ved

$$K_{\mathcal{D}} = (n_B, d_B) = (3233, 407).$$

Den første udregning der skal udføres er derfor

$$\mathcal{D}(0255) \equiv 0255^{407} \pmod{3233}.$$

Dette tal kan udregnes med samme metode som blev anvendt til (ind)krypteringen. Vi bemærker, at

$$\begin{aligned} 0255^{407} &= 0255^{256+128+16+4+2+1} \\ &= 0255^{256} \cdot 0255^{128} \cdot 0255^{16} \cdot 0255^{4} \cdot 0255^{2} \cdot 0255, \end{aligned}$$

og udregner følgende:

$$\begin{aligned} 0255^{1} \pmod{3233} &= 0255 \\ \\ 0255^{2} \pmod{3233} &= 65025 \pmod{3233} \\ &= 365 \\ \\ 0255^{4} \pmod{3233} &= 356^{2} \pmod{3233} \\ &= 133225 \pmod{3233} \\ &= 672 \\ \\ 0255^{8} \pmod{3233} &= 672^{2} \pmod{3233} \\ &= 451584 \pmod{3233} \\ &= 2197 \\ \\ 0255^{16} \pmod{3233} &= 2197^{2} \pmod{3233} \\ &= 4826809 \pmod{3233} \\ &= 3173 \\ \\ 0255^{32} \pmod{3233} &= 3173^{2} \pmod{3233} \\ &= 10067929 \pmod{3233} \\ &= 367 \\ \\ 0255^{64} \pmod{3233} &= 367^{2} \pmod{3233} \\ &= 134689 \pmod{3233} \\ &= 2136 \\ \\ 0255^{128} \pmod{3233} &= 2136^{2} \pmod{3233} \\ &= 4562496 \pmod{3233} \\ &= 733 \\ \\ 0255^{256} \pmod{3233} &= 733^{2} \pmod{3233} \\ &= 537289 \pmod{3233} \\ &= 611 \end{aligned}$$

Dekrypteringen af den første blok kryptotekst kan nu finde sted:

$$\begin{aligned}\mathcal{D}(0225) &\equiv 0255^{407} \pmod{3233} \\ &= 611 \cdot 733 \cdot 3173 \cdot 672 \cdot 365 \cdot 255 \pmod{3233} \\ &= 88882768802973600 \pmod{3233} \\ &= 1819.\end{aligned}$$

På lignende vis dekrypteres de resterende blokke kryptotekst og resultaterne bliver:

$$\begin{aligned}\mathcal{D}(1391) &\equiv 1391^{407} \pmod{3233} = 0110 \\ \mathcal{D}(1046) &\equiv 1046^{407} \pmod{3233} = 1118 \\ \mathcal{D}(1733) &\equiv 1733^{407} \pmod{3233} = 2516 \\ \mathcal{D}(1745) &\equiv 1745^{407} \pmod{3233} = 2005 \\ \mathcal{D}(1554) &\equiv 1554^{407} \pmod{3233} = 1809 \\ \mathcal{D}(1808) &\equiv 1808^{407} \pmod{3233} = 1407\end{aligned}$$

Disse kan nu sammensættes til tallet

$$181901001118251620051809 1407,$$

som ved hjælp af tabel 4.1 fra afsnit 4.1 oversættes tilbage til Alices besked til Bob: `RSA-KRYPTERING`.

Rivest, Shamir og Adleman brugte senere deres patent til at opbygge et firma som solgte RSA-løsninger til banker og andre virksomheder med brug for at kunne kommunikere sikkert. Adleman fortalte i interviewet med Bass fra 1995 også lidt om, hvordan dette spændte af.

> »Det var ligesom, 'Heh, vi bygger en high-tech industriel erhvervsvirksomhed i vores fritid'«, siger Adleman. Papirerne blev underskrevet i Adlemans Los Angeles lejlighed i 1982 – han var nu præsident af RSA Inc. Men hvordan var Adlemans indsats som forretningsmand så? Han kaster hovedet tilbage og griner. »I mine hænder røg forretningen lige i lokummet,« siger han. »Jeg var forfærdelig. Ligefrem horribel. Til sidst reorganiserede vi virksomheden og hyrede en rigtig præsident.« Han referer her til James Bidzos, som sluttede sig til RSA i 1986. Adleman er stadig aktionær og rådgiver i virksomheden hvis fremtid han ser som »relativt lovende«. (Bass; 1995, oversat fra engelsk)

Et år efter Bass' interview med Adleman blev virksomheden (RSA Data Security Inc.) solgt for ikke mindre end $200 millioner dollars.

4.4 Den ikke offentlige offentlige-nøgle kryptering

Når man taler om videnskabelige opdagelser eller opfindelser i historisk øjemed er der undertiden tale om to forskellige historier: Den offentligt tilgængelige og den *ikke* offentligt tilgængelige, eller med andre ord den der foregår på

universiteterne og den der foregår i sikkerhedstjenesterne. RSA og offentlig-nøgle kryptering er eksempler på videnskabelige resultater som netop har sådanne to forskellige historier. Vi har ovenfor hørt den offentlige historie som fandt sted på to amerikanske universiteter (Stanford og MIT), nu skal vi høre den ikke offentlige historie som fandt sted i den britiske sikkerhedstjeneste – en historie som ikke blev offentliggjort førend i 1997.[1]

Ifølge den britiske regering blev såvel offentlig-nøgle kryptering som RSA oprindelig opfundet ved Government Communications Headquaters (GCHQ) i Cheltenham, hvilket var en tophemmelig afdeling dannet efter anden verdenskrig ud fra resterne af Bletchley Park. Som vi har set i kapitel 1 begyndte problemet med distribution af private nøgler til (ind)kryptering og dekryptering at blive et problem i årene efter anden verdenskrig, hvor kryptering af information blev mere og mere udbredt og almindeligt. Militære organisationer var nogle af de få som rent faktisk kunne og hidtil havde været i stand til at betale de omkostninger der var forbundet med sikker kommunikation. Imidlertid begyndte det britiske militær i løbet af 1960erne at lege med ideen om at soldater skulle være udstyret med miniature-radioer og på den måde være i konstant kontakt med deres overordnede. Fordelene ved et sådant kommunikationssystem var åbenlyse, men problemet var at samtalerne blev nødt til at være krypterede i fald fjenden skulle finde på at lytte med. Med symmetrisk kryptering, som var den eneste tilgængelige form for kryptering på dette tidspunkt, ville et sådant system betyde at hver soldat skulle have sin egen private nøgle og ikke mindst, at hver af disse nøgler skulle distribueres på sikker vis. Militæret forudså, at enhver form for senere udvidelse af sådanne systemer ville være underlagt problemet med distribution af nøgler, og det i en sådan grad at udvidelser med rimelighed kunne anses som værende på det nærmeste umulige. Af den årsag blev en af GCHQs bedste krytografer bedt om at overveje situationen.

Kryptografen var James Ellis (1924-1997) som var uddannet ingeniør og som tilhørte den specielle division Communications-Electronics Security Group (CESG) under GCHQ. Ellis var kendt som værende uhyre iderig og vældig skarp, men også uforudsigelig og på ingen måde en født teamworker. Forfatteren og matematikeren Simon Singh fik i et interview med en af Ellis' kollegaer, Richard Walton, følgende beskrivelse af Ellis:

> Han var en temmelig sær kollega, han passede ikke rigtig ind i den daglig rutine i GCHQ. Men når det drejede sig om at finde på nye ideer var han ganske exceptionel. Man blev undertiden nødt til at sortere noget skidt fra, men han var vældig innovativ og altid villig til at udfordre det ortodokse. Vi ville for alvor være i vanskeligheder, hvis alle i GCHQ var som ham, men vi kan tolerere en større andel af sådanne folk end de fleste andre organisationer. Vi finder os i et antal folk som ham. (Singh; 1999, side 281, oversat fra engelsk)

[1] Dette afsnit er baseret på Simon Singhs skildring af begivenhederne i GCHQ i 1960'erne og '70'erne (Singh; 1999, side 279-292).

Et af Ellis' store fortrin var at han var bekendt med udviklingen inden for adskillige videnskabelige discipliner. Han plejede jævnligt at pløje et utal af videnskabelige tidsskrifter igennem og hans skabe på GCHQ var fyldt med de mest mærkværdige og obskure videnskabelige publikationer. Ellis var på sin afdeling kendt som lidt af en 'nøddeknækker', og når hans kollegaer havde problemer kom de ofte til ham i håb om, at hans viden såvel som hans hittepåsomhed kunne foranledige løsninger. Da Ellis fik til opgave at kigge på problemet med nøgle-distribuering var hans første skridt da også at betragte problemet fra en ny synsvikel. Ifølge Richard Walton ville Ellis altid, når han betragtede et problem, spørge: »Er dette virkelig, hvad vi ønsker at gøre?« Walton fortsætter: »Eftersom James var James, var en af de første ting han gjorde at udfordre kravet om, at det var nødvendigt at dele hemmelige data, med hvilket jeg mener nøglen. Der var ingen matematisk sætning som sagde, at man blev nødt til at dele en hemmelighed. Dette var noget som kunne udfordres.« Ellis gik på jagt i sine skabe fyldt med videnskabelige publikationer og fandt her en rapport fra Bell Telephone Laboratories stammende fra anden verdenskrig. Små tyve år senere gengav Ellis øjeblikket, hvor han indså at nøgle-distribuering ikke var uundgåelig del af kryptering som følger:

> Begivenheden som ændrede dette syn var opdagelsen af en Bell Telephone-rapport fra krigstiden af en ukendt forfatter som beskrev en sindrig ide for sikre telefonsamtaler. Den foreslog, at modtageren skulle maskere afsenderens tale ved at tilføje støj på linien. Han kunne fjerne støjen senere eftersom det var ham der havde tilføjet den og derfor vidste hvad det var. De åbenlyse praktiske ulemper ved dette system afholdt det fra rent faktisk at blive brugt, men det havde nogle interessante karakteristika. Forskellen mellem dette og konventionel kryptering er at i dette tilfælde tager modtageren del i (ind)krypteringsprocessen... Så var ideen født. (Singh; 1999, side 282, oversat fra engelsk)

Ideen er altså, at modtageren med vilje forårsager støj på linien eller *kommunikationskanalen*, som det også kaldes. *Støj* er et teknisk begreb for forstyrrelser på kommunikationskanalen. Normalt bliver støjen forårsaget af naturlige fænomener såsom atmosfæriske forstyrrelser og lignende og sådanne former for støj forekommer ofte på ganske tilfældig vis, hvilket gør det umuligt at korrigere for (med mindre afsender og modtager anvender en anden teknologi kendt som fejlkorrigerende koder). Ideen fra forfatteren ved Bell Telephone Laboratories var altså, at modtageren, Alice, skulle tilføje støj til kommunikationskanalen samtidig med at hun målte støjen. Afsenderen, Bob, fremsiger nu sin besked i telefonen over den støjbehæftede linie. Hvis en fremmed, Eve, lytter med på linien vil denne ingenting få ud af det grundet støjen på linien. Alice derimod kender jo naturen af støjen og kan i sin ende af linien fjerne den støj hun selv har påhæftet samtalen. Altså, har der her fundet en 'krypteret' form for kommunikation sted uden at Alice og Bob på noget tidspunkt har udvekslet nøgler. Kun Alice behøver at have kendskab til nøglen, det vil sige den målte natur af støjen. Ellis fortsætter sin beskrivelse således:

> Det næste spørgsmål var et åbenlyst et? Kan dette gøres med al-

> mindelig (ind)kryptering? Kan vi producere en sikker (ind)krypteret besked, læselig for den autoriserede modtager uden nogen form for tidligere hemmelig udveksling af nøgler? Spørgsmålet kom til mig en aften da jeg lå i min seng, og beviset for den teoretiske mulighed tog mig kun få minutter at udføre. Vi havde en eksistenssætning. Det utænkelige var rent faktisk muligt. (Singh; 1999, side 283, oversat fra engelsk)

Ellis' ide var ikke langt fra den af Diffie og Hellman, men dog med den markante forskel at han fik sine i slutningen af 1969, hvor forskere fra Stanford først fik deres i 1975. Ellis viste, at offentlig-nøgle kryptering – eller ikke-hemmelig kryptering, som han kaldte det – var muligt og han udviklede konceptet om separate offentlige- og private-nøgler. Men eftersom Ellis arbejdede for den britiske regering var han underlagt et løfte om tavshed og hans arbejde var af den grund kun kendt i GCHQ-regi, verden udenfor var uvidende om hans gennembrud inden for kryptografien. Ellis var således klar over, at han for at realisere sin ide måtte finde en matematisk envejsfunktion som opfyldte kravene til hans ikke-hemmelige kryptering, en envejsfunktion som han i kraft af sit eksistensbevis vidste måtte findes. Ellis selv var ikke den store matematiker og han indså snart at identificeringen af en sådan speciel envejsfunktion lå uden for hans rækkevidde. Ellis præsenterede ideen for sine overordnede og ideen blev bekræftet af andre af GCHQs medarbejdere.

De næste tre år forsøgte de kvikkeste hoveder i GCHQ så at finde en envejsfunktion som opfyldte Ellis' krav, men forehavendet lykkedes ikke. Ikke før i september 1973 i al fald hvor en ny matematiker fik ansættelse på afdelingen. Han hed Clifford Cocks og kom fra Cambridge, hvor han havde specialiseret sig i talteori. Cocks vidste imidlertid så godt som intet om kryptering og militær kommunikation, hvorfor en af hans nye kollegaer, Nick Patterson, fik til job at guide Cocks igennem hans første uger hos GCHQ. Efter seks uger fortalte Patterson Cocks om en »virkelig tosset ide«.

James Ellis (1924-1997)

Clifford Cocks

Patterson beskrev overfor Cocks Ellis' ide om offentlig-nøgle kryptering og fortalte samtidig at ingen havde været i stand til at finde en envejsfunktion som opfyldte kravene. Patterson fortalte denne historie til Cocks fordi Ellis' ide var den vildeste ide inden for kryptografi, ikke fordi han forventede at Cocks skulle kaste sig over den. Imidlertid var det netop hvad Cocks gjorde, og det allerede senere samme dag. Cocks fortæller selv:

> Der foregik ikke noget særligt, så jeg tænkte at jeg ville kigge lidt nærmere på ideen. Fordi jeg havde arbejdet med talteori var det naturligt at tænke på envejsfunktioner, noget man ikke kunne ændre tilbage. Primtal og faktorisering var en naturlig kandidat, og det blev mit startpunkt. [...] Fra jeg begyndte til jeg var færdig, tog det mig ikke mere end en halv time. Jeg var ret godt tilfreds med mig selv. Jeg tænkte, »Ooh, det er da fint. Jeg fik et problem, og jeg har løst det.« (Singh; 1999, side 284-285, oversat fra engelsk)

Hvad Patterson ikke havde fortalt Cocks var at GCHQs dygtigste matematikere havde ledt efter en sådan envejsfunktion i tre år, og Cocks havde derfor ingen ide om hvilken betydningsfuld opdagelse han havde gjort. Patterson derimod var helt på det rene med, hvad Cocks havde udrettet og fremlagde snart Cocks ide for ledelsen sammen med sin egen diskussion af de tekniske spørgsmål som uundgåeligt ville opstå. Herefter begyndte folk som Cocks slet ikke kendte at lykønske ham; vidunderbarnet som havde løst det tre år gamle problem som ingen andre havde kunne klare. En af disse for Cocks fremmede mennesker var James Ellis som var glad for endelig at se sin ide realiseret. Cocks havde imidlertid på dette tidspunkt stadig ikke helt indset betydningen af sin opdagelse og mødet med Ellis indprentede sig derfor ikke i hans hukommelse, hvorfor vi ikke kender Ellis' umiddelbare reaktion dengang på Cocks opdagelse. Cocks mindes dog, at han på det tidspunkt hvor betydningen af hans opdagelse gik op for ham tænkte, at dette her nok ville have skuffet G. H. Hardy en hel del.

Til trods for at Ellis og Cocks havde fundet på henholdsvis offentlig-nøgle krypteringen og en måde at implementere denne på, så var deres ideer underlagt den begrænsede computerkraft som fandtes i begyndelsen af 1970'erne. Selv om computerne på dette tidspunkt var udmærkede i stand til at håndtere symmetriske kryptosystemer som DES, så var et asymmetrisk system som RSA en anden sag. En implementering af RSA krævede væsentlig mere computerkraft end der var til stede i 1973 og GCHQ var derfor ikke i stand til at føre Ellis' og Cocks' ideer ud i livet. Ideerne var simpelthen en fem til ti år forud for deres tid. I begyndelsen af 1974 blev en af Cocks gamle skolekammerater og kollegaer fra Cambridge university, Malcolm Williamson, også ansat ved GCHQ. Cocks, som tidligere kun havde været i stand til at fortælle sin kone om sin opdagelse, idet hun også arbejdede ved GCHQ, berettede nu om Ellis' og sin egen ide til Williamson. Denne var dog yderst skeptisk: »Cliff forklarede hans ide til mig«, husker Williamson, »og jeg troede ikke rigtigt på det. Jeg var meget mistænksom, for det er en meget besynderlig ting at være i stand til.« Williamson følte sig overbevist om, at Cocks måtte have lavet en fejl og han satte sig for at bevise dette. Forsøget

på at modbevise Cocks ide mislykkedes, men tilgengæld fandt Williamson i forsøget den præcis samme metode til offentlig nøgle-udveksling som forskerne fra Stanford (den såkaldte Diffie-Hellman-Merkle nøgle-udveksling, se opgave 72) og det tilmed omtrent samtidig med at Martin Hellman fandt den.

Ellis, Cocks og Williamson havde altså i begyndelsen af 1975 gjort samtlige af de opdagelser som i løbet af de næste tre år skulle komme til at udgøre offentlig-nøgle kryptering, og det eneste de kunne gøre var at se til mens forskerne fra Stanford og MIT løb med laurbærrene og fik al berømmelsen. Cocks og Williamson lod dog ikke til at tage dette særligt ilde op, i Singhs interview med dem siger Williamson: »Min reaktion var: 'Okay, sådan er det bare.' I bund og grund fortsatte jeg bare med resten af mit liv.« Cocks påpeger følgende: »Man involverer sig ikke i dette [sikkerhedstjenesten] for at få offentlig anerkendelse.« Det eneste Williamson ifølge Singh fortryder er, at GCHQ ikke formåede at tage patent på offentlig-nøgle kryptering. Men i begyndelsen af 1970'erne havde GCHQ for det første en politik om ikke at tage patenter, da dette ville betyde at organisationen i et vist omfang ville blive nødt til at afsløre, hvad de gik og lavede. For det andet var det uklart om man overhovedet kunne tage patenter på algoritmer, men det blev stadfæstet i 1976 da Diffie og Hellman søgte om et og atter i 1977 da Rivest, Shamir og Adleman gjorde. For det tredje var ledelsen af GCHQ nok bare ikke ligeså fremsynede som forskerne fra Stanford og MIT med hensyn til computerens udbredelse og de behov Internettet ville føre med sig. GCHQ stod altså fuldstændig udenfor indflydelse på udviklingen af offentlig-nøgle kryptering.

Selv om GCHQs arbejde med offentlig-nøgle kryptering var hemmeligt var der en anden organisation som var bekendt med Ellis', Cocks' og Williamsons resultater, og det var NSA. Og formentlig var det netop via NSA at Diffie hørte rygterne om det britiske arbejde. I hvert fald drog Diffie i 1982 til Cheltenham for at se om der var hold i rygterne. Her mødtes han med Ellis og forsøgte gentagne gange at få klar besked, hvilket ikke var nemt da Ellis tog sit tavshedsløfte alvorligt. Efter sigende gik Diffie dog til sidst lige i kødet på Ellis og sagde: »Fortæl mig om hvordan du opfandt offentlig-nøgle kryptering?«, hvortil Ellis efter en lang pause hviskede: »Jeg ved ikke hvor meget jeg burde sige. Men lad mig sige, at I gjorde meget mere med det end vi gjorde.« Og netop denne udtalelse fra Ellis indeholder måske en vis pointe. For selv om den britiske sikkerhedstjeneste var de første til at finde på offentlig-nøgle kryptering og RSA, så var det akademikerne der forstod potentialet af ideen og som formåede at implementere dem. Dertil kommer at akademikerne formåede at nå de samme resultater som sikkerhedstjenesten ganske uden at kende til dennes arbejde. Singh bemærker underholdende nok i sin bog, at selve 'informationsflowet' mellem offentlige og ikke-offentlige instanser som for eksempel universiteterne og sikkerhedstjensterne i sig selv repræsenterer en envejsfunktion; information flyder frit fra universiteterne til sikkerhedstjensterne, men flowet i modsat retning er umuliggjort af forbud. Til sidst bør nævnes, at hvis ikke offentlig-nøgle kryptering var blevet til som en offentlig tilgængelig akademisk disciplin havde hemmeligheden sikkert stadig være velbevaret i sikkerhedstjensterne (citatet af Ellis på side 106 synes

at bekræfte en sådan formodning). Dette ville have betydet, at vi i dag ikke havde været i stand til at udnytte for eksempel Internettet i samme grad og omfang som vi nu er vant til.

Cocks fik i 1997 lov af GCHQ til i et foredrag at offentliggøre sit og Ellis' arbejde med offentlig-nøgle kryptering og RSA. Dette skete den 18. december, mindre end en måned efter at Ellis var død, den 25. november, i en alder af 73 år.

4.5 Anvendelser, sikkerhed og fremtid

RSA bruges i dag i så udbredt grad på Internettet, at det næsten er umuligt at forestille sig nettet uden RSA. Eksempelvis bruges RSA til online bankforretninger såvel som autentification i forbindelse med e-handel og andre pengetransaktioner over nettet. RSA er derudover en indkorporeret del af diverse industrielle koncerners computernetværk, internt såvel som eksternt, eksempelvis annoncerer Rolls Royce & Bentley Motor Cars deres brug af RSA på nettet. Og det er ikke kun i forretningssammenhæng, at RSA bruges til at sikre såvel kommunikationen indadtil som udadtil, diverse regeringer og disses sikkerhedstjenester benytter sig i mindst lige så høj grad af algoritmen. RSA-softwareløsninger findes i dag i utallige afskygninger, hver især matchende netop de specifikke behov, som en given organisation, statslig såvel som privat, måtte have. Udover brugen af RSA i forbindelse med Internettet bruges RSA selvfølgelig også i alle mulige andre sammenhænge, hvor sikker kommunikation er påkrævet, eksempelvis hver gang vi benytter et kreditkort.

Den omfattende udbredelse af RSA gør det naturligvis attraktivt for 'skumle personager' at forsøge at knække diverse implementeringer af algoritmen. Vi har allerede tidligere berørt visse af de sikkerhedsmæssige aspekter af RSA i forbindelse med den tidskrævende proces det er at primfaktorisere meget store heltal, i RSAs tilfælde at faktorisere n i p og q. Men findes der andre måder at knække algoritmen på? Den offentlige nøgle for RSA består som tidligere set af heltallene n og e. De private parametre omfatter udover d, som udgør halvdelen af den private nøgle, også p, q og $\phi(n)$. Kender man enten p eller q kan man hurtigt beregne det andet primtal ved at dividere det kendte op i n, og når man først kender primfaktoriseringen af n kan man beregne $\phi(n) = (p-1)(q-1)$, udfra hvilken den private nøgle d er fastlagt. Da d bestemmes udfra e og $\phi(n) = (p-1)(q-1)$ er $\phi(n)$ altså mindst lige så vigtig at holde hemmelig som p og q selv. En angriber på et RSA-kryptosystem kan knække dette, hvis han eller hun kender enten d, $\phi(n)$, p eller q. Altså er det ikke nok at hemmeligholde p og q selv, informationer *om* p og q og disses indbyrdes forhold må også hemmeligholdes. Kender en angriber eksempelvis enten $(p+q)$ eller $(p-q)$ viser det sig, at man udfra denne viden er i stand til at beregne $\phi(n)$, og derfra som ovenfor set bryde kryptosystemet (se opgaver 70 og 71). Selve $\phi(n)$ kendes der dog ingen metoder til at beregne udover at kende p og q selv, så hvis blot man hemmeligholder disse og informationer om dem skulle man kunne føle sig sikker overfor angreb anvendende $\phi(n)$. Det

efterlader os med de tre resterende private parametre d, p og q. Hvilke krav stilles der til disse for at opretholde sikkerheden af RSA? Det viser sig, at hvis disse blot vælges såvel 'store nok' som med omtanke, så kendes der pt. ikke nogen metoder til at beregne disse inden for en overskuelig tidsramme. Men hvad vil det sige at vælge sine parametre med omtanke? Fra sætning 2.29 ved vi, at vi for at bestemme primfaktorerne i et heltal n 'kun' behøver at forsøge os med primtallene op til $\sqrt{n}$, det vil sige dem i listen $2, 3, 5, 7, \ldots, \sqrt{n}$ (hvor $\sqrt{n}$ jo ikke nødvendigvis er et primtal, eller for den sags skyld et heltal). Et sådant 'brute force'-angreb kan man ikke gardere sig imod, men man kan trække det ud. For det første bør man ikke vælge primtal som enten er for små eller ligger for tæt på $\sqrt{n}$, da det vil være naturligt for en angriber at begynde i henholdsvis den ene eller den anden ende af listen. Samtidig må afstanden mellem primtallene heller ikke være for lille. Oftest vælger man to primtal sådan at disse har samme størrelsesorden, det vil sige samme antal cifre, men størst mulig afstand. Et eksempel på dette er primtallene 1009 og 9973, disse er af samme størrelsesorden, men der er stor afstand imellem dem. Og så skal de som sagt være 'store nok', og hvis p og q er store nok, så vil d også være det, da denne parameter jo afhænger af p og q. Men hvad vil det så sige at p og q er store nok? Faktisk afhænger dette mål i høj grad af den teknologi som er tilgængelig til et givet tidspunkt. De størrelsesordner som man kunne nøjes at operere med i 1982, hvor Rivest, Shamir og Adleman oprettede deres firma, vil langt fra være tilstrækkelige i dag. I 1995 udregnede sikkerhedseksperten Simon Garfinkel, at det ville tage en computer med 8 MB RAM cirka 50 år at faktorisere et n af størrelsesorden 10^{130}, svarende til at p og q hver er af størrelsesorden 10^{65}. Imidlertid udregnede Garfinkel også, at 100 millioner sådanne computere, hvilket var det antal der var solgt i 1995, ved distribuerede beregninger kunne faktorisere et sådant n på 15 sekunder. Sådanne distribuerede beregninger er som vi så i afsnit 2.4 med GIMPS ikke blot fantasi. Eksempelvis blev Gardners 129 cifre lange heltal fra 1977 (se side 79) faktoriseret i 1994 netop ved en koordineret indsats mellem sekshundrede talentusiaster anvendende pc'er. Primtallene p og q var på henholdsvis 64 og 65 cifre. På dette tidspunkt blev der til vigtige banktransaktioner anvendt n'er mindst af størrelsesorden 10^{308}. Dette er imidlertid over et årti siden og i dag er kravet grundet den teknologiske udvikling noget højere.

På samme måde som man kan tale om et 'kapløb' mellem kryptografer og kryptoanalytikere, synes der også at være tale om et 'kapløb' mellem matematikken og teknologien – tænk eksempelvis på Enigmaens fremkomst og derefter computerens. For RSAs vedkommende har matematikken dog indtil videre været i stand til at bevare sin førerposition ved at skrue op for antallet af cifre i den offentlig nøgle. Spørgsmålet er dog om dette kan fortsætte. Det er nemlig ikke kun teknologien som matematikken her løber om kap med, i en vis forstand løber den også om kap med sig selv. Hele tiden bliver der forsket i nye metoder og algoritmer til faktorisering af store heltal. Skulle en sådan metode pludselig dukke op ville RSA ikke længere være et sikkert kryptosystem. Mange matematikere er dog af den opfattelse at faktorisering er en så speciel og vanskelig opgave, at der må være en eller anden matematisk lov som forbyder at der kan tages genveje. Måske har

de ret, i hvert fald har matematikere i løbet af de sidste par tusinde år ikke fundet nogen metode som løser problemet. Men som mundheldet siger skal man aldrig sige aldrig. Et andet meget besværligt problem i talteorien er, som vi har diskuteret tidligere, det at teste om et givet heltal er et primtal. I 1970erne tog det med de mest effektive algoritmer 10^{44} år at teste om et tal på 1000 cifre var et primtal. Men i 1980 skete der et skred på dette område, da vores gode bekendte Adleman sammen med en anden matematiker ved navn Robert Rumely fandt en effektiv test som kunne teste, hvorvidt tal på 1000 cifre var primtal eller ej på blot én uge. Talteoretikeren Carl Pomerance skrev i 1982, samme år som Rivest, Shamir og Adleman oprettede deres firma, i denne forbindelse følgende:

> Udviklingen i primtalstestning har ingen direkte betydning for problemet omhandlende faktorisering, men på den anden side så har ingen vist at faktorisering ikke lader sig løse. Der er ingen garanti for at en eller anden ikke vil opfinde en revolutionerende metode til faktorisering i morgen. Derfor bør en beslutning om sikkerheden på længere sigt af offentlig-nøgle systemer som baserer sig på problemet med faktorisering træffes udfra en subjektiv vurdering af om der vil eller ikke vil forekomme fremskridt med hensyn til faktorisering. Den nylige udvikling i testen for primtal tjener til at fremhæve den potentielle sårbarhed af en sådan kode [kryptering] overfor et teoretisk gennembrud. (Pomerance; 1982, side 130, oversat fra engelsk)

Pomerance var altså skeptisk, eller blot håbefuld med hensyn til udviklingen af talteorien, men her mere end to årtier efter er faktorisering af tilstrækkeligt store heltal stadig en uoverkommelig opgave for såvel teknologien som matematikken selv, og RSA-kryptering vurderes stadig som værende sikker. Store koncerner som eksempelvis AT&T og Hewlett-Packard, hvis teknologi og ydelser i høj grad baserer sig på sikkerheden af RSA, holder dog hele tiden et vågent øje med matematikkens udvikling inden for området. Sådanne organisationer er selvfølgelig interesserede i, at deres systemer altid er up-to-date med hensyn til sikkerhed, og ny talteoretisk indsigt i primtallenes underfundige natur kunne gå hen og stille nye krav til RSA og måske endda offentlig-nøgle kryptering i det hele taget. Da der i 1997, som følge af en aprilsnar der var løbet løbsk, florerede et usandt rygte i den matematiske verden om at Rieman-hypotesen var blevet bevist var diverse industrielle koncerner – såvel som NSA – straks på pletten for at få et overblik over eventuelle følger, eksempelvis for e-handlen.

Kryptografiens historie har indtil videre vist, at et hvert 'ubrydeligt' kryptosystem før eller siden må lade livet som følge af enten udviklinger inden for teknologien eller inden for matematikken. I dag fører matematikken kapløbet over teknologien, men som kryptografiens historie også viser har det ikke altid været sådan. Enigmaen var jo netop et eksempel på, at teknologien i et vist tidsrum tog førertrøjen fra matematikken, i hvert fald indtil de polske, og senere de engelske, matematikere fik bugt med denne tyske kode. Efterfølgende var det matematikerne der var i stand til at tage næste skridt ved at løse nøgle-distribueringsproblemet og skabe RSA, et nyt sikkert kryptosystem. Til

realiseringen af dette anvendte de selv den teknologi, den digitale computer, som de nu løber om kap med for at opretholde sikkerheden af RSA. Det nærliggende spørgsmål er, hvad teknologiens næste træk bliver. Vil der ske en eller anden revolutionerende udvikling inden for teknologien, således at denne kommer foran eller slet og ret vinder kapløbet med matematikken? En sådan udvikling diskuteres i nogen grad allerede med den såkaldte *kvantecomputer*. Kvantecomputeren er en computer som baserer sig på fysikkens kvanteteori, en teori vi ikke skal forsøge at beskrive her. Derimod skal vi pointere et par af konsekvenserne af en sådan computers eksistens. Kvantecomputeren findes nemlig ikke endnu i en velfungerende udgave. Men det gør til gengæld programmer til den – programmer, som hvis den nogensinde skulle blive en realitet, kan faktorisere heltal en million gange større end Gardners 129 cifrede heltal på få sekunder. Programmer til brydning af RSA og andre kryptosystemer som for eksempel DES er allerede skrevet, blandt andet af forskere ved Bell Laboratories, og ligger blot og venter på at kvantecomputeren skal manifestere sig. Men kryptograferne er dog på forkant med situationen, idet en ny form for kryptering, den såkaldte *kvantekryptering*, også blot ligger og venter på at kvantecomputeren skal blive til virkelighed. Og sådan fortsætter kapløbet mellem matematikken og teknologien ligesom kapløbet mellem kryptograferne og kryptoanalytikerne. Hvem der vinder er ikke til at sige, men at det vil vare længe førend de to kapløb er forbi, hvis overhovedet nogensinde, synes derimod sikkert – så sikkert som noget som helst inden for kryptografien nu engang kan være.

4.6 Opgaver

Opgave 56
Opskriv formlen, $\mathcal{C}^{-1}(y)$, for dekryptering af Cæsar-kryptering.

Opgave 57
Modificer opskrivningen i afsnit 1.4 af Cæsar-kryptering (inklusiv dekryptering) som algoritme ved at bruge formlerne baseret på modulo-regning.

Opgave 58
Opskriv formlerne for Cæsar-kryptering og -dekryptering, hvor vi i stedet for tallet 3 kan benytte et vilkårligt tal k. Hvilken betingelse giver det mening at lade k opfylde? Benyt formlen med $k = 7$ til at (ind)kryptere beskeden `OGSÅ DU MIN SØN BRUTUS`.

Opgave 59
Cæsar-kryptering hvor man kun forskyder bogstaverne frem i alfabetet udgør ikke en særlig sikker metode til kryptering. Hvorfor?

En lidt anderledes, omend ikke meget mere sikker metode, kan opnås ved at benytte formlen

$$\mathcal{C}(x) = (ax + b) \text{ modulo } 30.$$

Oversæt beskeden `TERNINGERNE ER KASTET` med værdierne $a = 2$ og $b = 3$.

Opgave 60
Opskriv $\mathcal{C}^{-1}(y)$ for $\mathcal{C}(x) = (2x + 3)$ modulo 30, og dekrypter den krypterede besked fra forrige opgave (opgave 59).

Opgave 61
Forklar med dine egne ord RSA-algoritmen.

Opgave 62
Forklar hvad der i RSA forstås ved følgende: n, p, q, M, C, $K_{\mathcal{E}}$, $K_{\mathcal{D}}$, d, $\mathcal{E}(M)$, $\mathcal{D}(M)$, $K_{\mathcal{E}} = (n_A, e_A)$, $K_{\mathcal{E}} = (n_B, e_B)$, $K_{\mathcal{D}} = (n_A, d_A)$, $K_{\mathcal{D}} = (n_B, d_B)$.

Opgave 63
Forklar hvad der i RSA forstås ved følgende udtryk, hvor de indgår i algoritmen samt hvad deres formål er:

- $n = p \cdot q$,
- $\text{sfd}(e, \phi(n)) = 1$,
- $\text{sfd}(e, (p-1)(q-1)) = 1$,
- $C \equiv \mathcal{E}(M) \equiv M^e \pmod{n}$,
- $ed \equiv 1 \pmod{(p-1)(q-1)}$,
- $\mathcal{D}(C) \equiv C^d \pmod{n}$.

Opgave 64
Med udgangspunkt i opgave 61 tegn da en figur af, hvordan RSA fungerer (jævnfør eventuelt figur 1.2). Påfør dernæst, med udgangspunkt i opgaverne 62 og 63, de forskellige parametre og formler på figuren.

Opgave 65
Med udgangspunkt i $K_{\mathcal{E}} = (n_A, e_A)$, $K_{\mathcal{E}} = (n_B, e_B)$ og $K_{\mathcal{D}} = (n_A, d_A)$, $K_{\mathcal{D}} = (n_B, d_B)$ beskriv da en situation, hvor Alice først sender en RSA-krypteret besked til Bob og hvor Bob bagefter sender en RSA-krypteret besked tilbage til Alice.

Opgave 66
Formuler den i afsnit 4.3 anvendte modulo-udregning af tal med store potenser som en algoritme.

Opgave 67
RSA-krypter eller -dekrypter følgende beskeder med de i afsnit 4.3 anvendte parametre:

a. `RIVEST`
b. `SHAMIR`
c. `0774 0486 1515`.
d. `1533 1695 0416`.
e. `0396 0083 1884`.
f. `2844 2760 2354`.

Opgave 68
I afsnit 4.3 anvendte vi sammen med $p = 53$ og $q = 61$ e-værdien 23. Imidlertid er valget af e ikke entydigt.

a. Godtgør ved hjælp af Euklids algoritme at $e = 17$ også opfylder de givne krav, altså at $\text{sfd}(e, \phi(n)) = \text{sfd}(17, 3120) = 1$.
b. (Ind)krypter beskeden `RIVEST` ved brug af den offentlige nøgle $K_{\mathcal{E}} = (3233, 17)$.
c. (Ind)krypter beskeden `SHAMIR` ved brug af den offentlige nøgle $K_{\mathcal{E}} = (3233, 17)$.

Opgave 69
Når vi i opgave 68 har udskiftet e-værdien i den offentlige (ind)krypteringsnøgle, må vi også udskifte d-værdien i den private dekrypteringsnøgle.

a. Arbejd dig baglæns igennem Euklids algoritme for $\text{sfd}(17, 3120)$ for at bestemme værdien af d.
b. Dekrypter beskeden `2770 1471 1542` ved brug af den private nøgle $K_{\mathcal{D}} = (3233, d)$.
c. Dekrypter beskeden `0572 1695 0416` ved brug af den private nøgle $K_{\mathcal{D}} = (3233, d)$.

Opgave 70
Hvis man kender $p + q$ kan $\phi(n)$ beregnes ved at trække $p + q$ fra n og lægge 1 til. Med udgangspunkt i $\phi(n) = (p - 1)(q - 1)$ vis da dette.

Opgave 71
Hvis man kender $p - q$ kan man udregne $\phi(n)$ fra $p - q$ ved formlen:

$$\phi(n) = (n + 1) - \sqrt{(p - q)^2 - 4n}.$$

Med udgangspunkt i resultatet fra opgave 70 vis da, hvordan man kommer frem til denne formel. (Vink: Du skal benytte dig af tricket med at omskrive $p + q$ til $\sqrt{(p + q)^2}$ samt at skrive $2pq$ som $-2pq + 4pq$.)

Opgave 72
Diffie-Hellman-Merkel nøgle-udveksling (se beskrivelsen i afsnit 1.3) baserer sig på følgende matematiske envejsfunktion:

$$Y^x \pmod{P},$$

hvor Y og P, med $Y < P$, er de to parameterværdier Alice og Bob aftaler til at begynde med. Antag, at Alice og Bob aftaler parametrene $Y = 7$ og $P = 11$ og at Alice derefter vælger sin hemmelige x-værdi, tidligere kaldet a, til at være 3 og at Bob sætter sin, tidligere kaldet b, til at være 6.

a. Udregn nu henholdsvis Alices og Bobs udtryk: $7^3 (\text{mod} 11)$ og $7^6 (\text{mod} 11)$.

Alice og Bob udveksler nu deres resultater, tidligere kaldet α og β, og udregner henholdsvis $\beta^3 \pmod{11}$ og $\alpha^6 \pmod{11}$.

b. Udregn disse.

På 'mirakuløs' vis er Alices og Bobs resultat det samme, og det er dette tal, tidligere kaldet γ, som udgør deres fælles private nøgle – en privat nøgle som de har udvekslet uden at have været nødt til at mødes og uden at Eve har haft en mulighed for at opsnappe den.

c. Vis, ved at betragte de to generelle udtryk $Y^a \pmod{P} = \alpha$ og $Y^b \pmod{P} = \beta$ at Alice og Bob nødvendigvis må få det samme γ når de udfører beregningerne i opgave b. Gør derefter 'prøve' med de i opgaverne a og b benyttede talværdier.

5 Afsluttende essay-opgave

Den afsluttende opgave er en længere, mere krævende og mere omfattende (essay-)opgave som der arbejdes med over et antal lektioner. Den afsluttende opgave (opgave 73) består fortrinsvist af to delopgaver (73a og 73b) samt en række mindre essay-opgaver (opgaver 74, 75, og 76), hvis formål det er at yde støtte til besvarelsen af opgave 73 og som skal løses *før* besvarelsen af denne. (Bemærk, at man for at besvare essay-opgave 74 skal have læst G. H. Hardys *A Mathematician's Apology*.) Derudover tjener de tidligere besvarede historiske opgaver (45, 46 og 55) også i nogen grad som støtte til besvarelsen af den afsluttende opgave. Det er vigtigt, at I læser teksten til den afsluttende opgave (73), inden I går igang med de øvrige essay-opgaver, således at I kan gøre jer klart, hvad I skal bruge disse til i besvarelsen af opgave 73.

Opgave 73 afleveres skriftligt og besvarelser af essay-opgaverne (74, 75 og 76) vedlægges som bilag til besvarelsen af opgave 73. Hvis I anvender informationer fra Internettet skal de anvendte web-sites angives. God fornøjelse!

5.1 Matematikhistorieskriving

Når man beskæftiger sig med historie og historisk forskning kan man have mange forskellige indgangsvinkler til eller syn på dette. Sådanne forhold gør sig selvfølgelig også gældende inden for matematikhistorie og matematikhistorisk forskning. Eksempelvis kan man udelukkende interessere sig for *hvornår* hvad skete og *hvem* der fik det til at ske. En sådan tilgang til matematikhistorien vil handle meget om, at fastsætte datoer for fremkomsten af forskellige begreber, sætninger, discipliner og teorier og tilskrive disse til forskellige matematikere – et studie af hvem der i virkeligheden kom først med hvad. En anden tilgang kan gå ud på at bestemme *hvorfor* en bestemt udvikling inden for matematikken fandt sted og *hvordan* denne udvikling forløb.

Opgave 73 (Afsluttende essay-opgave)
Med jeres nuværende kendskab til offentlig-nøgle krypteringens historie, RSA og den talteori som RSA baserer sig på bedes I give to fremstillinger af historien:

a. En fremstilling der udelukkende baserer sig på *hvornår* og *hvem*. Elementer af jeres diskussion i essay-opgave 76 bør indgå i denne fremstilling.
b. En anden fremstilling der baserer sig på *hvorfor* og *hvordan*. I bedes blandt andet forsøge at beskrive, hvad der har dikteret fremkomsten

og udviklingen af offentlig-nøgle kryptering og RSA. Elementer af jeres diskussioner i essay-opgaver 74 og 75 bør indgå i denne fremstilling, ligeledes bør elementer af de tidligere besvarede historiske opgaver 45, 46 og 55 indgå.

c. Hvis I tidligere har været igennem undervisningsforløbet om *Kodningsteoriens tidlige historie* forventes det også, at I i hvorfor-og-hvordan fremstillingen inddrager en diskussion af *genstande* og *behandlingsmåder* i udviklingen af RSA.

d. Hvilke indsigter i matematikkens historie mener I man kan få frem ved at belyse sin fremstilling af historien gennem indre og ydre drivkræfter?

e. Hvis I tidligere har været igennem undervisningsforløbet om *Kodningsteoriens tidlige historie* bedes I også diskutere, hvilke indsigter I mener, man kan få frem ved at betragte matematikkens historie i termer af genstande og behandlingsmåder.

f. Hvad synes I man kan lære af henholdsvis hvornår-og-hvem fremstillingen og hvorfor-og-hvordan fremstillingen.

5.2 Ren og anvendt matematik

For at besvare denne essay-opgave skal I læse matematikeren og talteoretikeren G. H. Hardys bog *A Mathematician's Apology* fra 1940. Hardy giver i denne bog udtryk for en hel del mere eller mindre radikale holdninger om matematik såvel som om matematikere. Det er meningen at I med jeres nuværende kendskab til matematikkens, herunder talteoriens og specielt krypteringens, historie skal diskutere visse af Hardys synspunkter.

Opgave 74 (Essay-opgave)
G. H. Hardy diskuterer i sin *A Mathematician's Apology*, hvad han forstår ved henholdsvis *ren* og *anvendt* matematik. Ligeledes giver han også udtryk for sine egne (personlige og politiske) holdninger til henholdsvis ren og anvendt matematik.

a. Redegør for, hvad Hardy karakteriserer som henholdsvis ren og anvendt matematik.

b. Hvad er Hardys syn på henholdsvis ren og anvendt matematik? Hvilke eksempler giver han i sine diskussioner heraf?

c. Diskuter Hardys udtalelser om talteori (se også afsnit 3.5) på baggrund af jeres kendskab til udviklingen af RSA. Eksempelvis, hvad fortæller tilfældet med RSA os om vigtigheden af (matematisk) grundforskning? Hvordan hænger dette sammen med Hardys udtalelser om talteori? (Og Nicholas Bernoullis udtalelse fra 1778 om Eulers arbejde?)

d. Hvad synes I generelt om Hardys *Apology* og det syn på matematik og matematikere som han lægger for dagen heri? I hvor høj grad tror I, at matematikere i dag deler Hardys meninger om de forskellige aspekter af matematikken som han diskuterer i sin bog?

5.3 Indre og ydre drivkræfter

Når man beskriver udviklingen af matematik skelner man undertiden imellem de indre og de ydre drivkræfter. Med *indre drivkræfter* menes de kræfter som driver den matematiske forskning indefra, eksempelvis de spørgsmål som matematikken søger at løse for den matematiske forsknings egen skyld. Tidligere eller stadig uløste problemer i talteorien som for eksempel Fermats sidste sætning, Goldbachs formodning og Riemann-hypotesen er eksempler på sådanne spørgsmål som driver den matematiske forskning fremad på de indre linier. Med *ydre drivkræfter* forstås derimod de kræfter som påvirker den matematiske forskning udefra. Eksempelvis er krig, som Hardy diskuterer, en ydre drivkræft for matematikken. Ofte har krige givet anledning til nye spørgsmål som efterfølgende er blevet løst af naturvidenskabsfolk ved at disse har udviklet nye områder inden for deres respektive felter, herunder matematikken. En hel klar ydre drivkræft i denne sammenhæng er penge. Anden verdenskrig og den efterfølgende kolde krig er eksempeler på 'begivenheder' i forbindelse med hvilke finansieringen af naturvidenskabelig og matematisk forskning blev øget kraftigt. Dette førte for matematikkens vedkommende til adskillige nye matematiske resultater, discipliner og teorier, såvel inden for ren som inden for anvendt matematik.

Opgave 75 (Essay-opgave)
Blandt forskere i matematikkens historie synes der i dag at være enighed om, at man for at beskrive udviklingen af et matematisk område eller en matematiske disciplin bør belyse såvel de indre som de ydre drivkræfter der har været i spil i denne udvikling. I den følgende opgave skal I gøre netop dette for RSA.

a. Med udgangspunkt i de i dette undervisningsmateriale præsenterede matematikere af ældre dato (Euklid, Sun Zi, Fermat, Euler, Gauss, Riemann, Hardy) diskuter da for hver af disse deres personlige motivation for at beskæftige sig med de dele af talteorien som de gjorde. Hvordan relaterer de enkeltes motivation sig til diskussionen af indre og ydre drivkræfter?
b. Med udgangspunkt i de i dette undervisningsmateriale præsenterede matematikere af nyere dato (Diffie, Hellman og Merkle; Rivest, Shamir og Adleman; Ellis, Cocks og Williamson) diskuter da for hver af disse deres personlige motivation for at beskæftige sig med de dele af krytografien og/eller talteorien som de gjorde. Hvordan relaterer de enkeltes motivation sig til diskussionen af indre og ydre drivkræfter?
c. Diskuter jeres svar af de to ovenstående spørgsmål om indre og ydre drivkræfter i forhold til hinanden.

5.4 Offentlig og ikke-offentlig forskning

Kryptografiens historie er et klasseeksempel på, hvordan meget forskning ofte foregår hemmeligt i regeringsregi. Og som historien med offentlig-nøgle kryptering og RSA viser hænder det undertiden også, at en sådan forskning foregår mere eller mindre parallelt med forskningen ved universiteterne. Af

hensyn til historieskrivningen kan det dog være relevant at få offentliggjort den hemmelige forskning, specielt hvis denne har haft en betydning for udviklingen af et givet felt, men måske også hvis den ikke har. I et indtil for nyligt hemmeligt skrift fra 1987 om opfindelsen af offentlig-nøgle kryptering i GCHQ-regi siger Ellis:

> Kryptografi er en højst usædvanlig videnskab. De fleste professionelle videnskabsfolk stiler mod at være de første til at publicere deres arbejde, fordi det er gennem udbredelse at arbejdet opnår sin værdi. Den højeste værdi af kryptografi opnås i modsætning hertil ved at minimere den tilgængelige information for potentielle modstandere. Professionelle kryptografer arbejder derfor normalt i lukkede samfund for på den måde at opnå et tilstrækkeligt professionelt arbejde til sikring af høj kvalitet samtidig med at hemmelighederne bevares overfor udenforstående. Afsløring af disse hemmeligheder tillades som regel kun af hensyn til historisk korrekthed, når det er sikkert, at der ikke længere kan opnås fordele ved at bevare hemmeligheden. (Singh; 1999, side 292, oversat fra engelsk)

Som beskrevet i afsnit 4.4 rejste Diffie til England for at tale med Ellis. Efter at være kommet tilbage til USA fortalte Diffie til Hellman at rygtet om, at GCHQ havde opfundet offentlig-nøgle kryptering før dem selv var sandt. Simon Singh genfortæller episoden sådan her:

> Da Diffie fortalte Hellman om Ellis, Cocks og Williamson var hans holdning at akademikernes opdagelser skulle være en fodnote i historien om den klassificerede forskning, og at GCHQs opdagelser skulle være en fodnote i historien om den akademiske forsking. Men på daværende stadie var der ingen udover GCHQ, NSA, Diffie og Hellman som kendte til den klassificerede forskning, og derfor kunne den ikke engang blive taget i betragtning til en fodnote. (Singh; 1999, side 290, oversat fra engelsk)

Opgave 76 (Essay-opgave)
Matematikkens historie byder på talrige eksempler af sætninger og andre matematiske resultater som er opkaldt efter andre matematikere end dem der rent faktisk fandt på dem. Eksempelvis kan man diskutere, hvem der rent faktisk formulerede Goldbachs formodning; Goldbach eller Euler. Selvfølgelig formulerede Euler den nuværende Goldbachs formodning på baggrund af Goldbachs oprindelige formodning, og sådan kan man så argumentere frem og tilbage... og det gør matematikhistorikere også indimellem.

En anden ting som der ofte er fokus på i matematikkens historie er, hvem der kom først med hvad. Heller ikke dette spørgsmål er altid lige nemt at svare på, da matematiske resultater kan optræde i mange forskellige sammenhænge, inden for såvel ren som anvendt matematik, og på mange forskellige måder. Også dette er noget som matematikhistorikere fra tid til anden bruger en hel del krudt på.

I skrivningen af den nyere matematikhistorie optræder de ovenstående problemer undertiden i en ny 'forklædning' som heller ikke letter forskningen

for matematikkens historikere. Denne forklædning består i den klassificerede forskning som udføres af diverse regeringers sikkerhedstjenester, forskning hvis omfang efter især anden verdenskrig er blevet forøget væsentligt.

a. Søg på Internettet og se hvad I kan finde af informationer om henholdsvis NSA og GCHQ (ved at søge på 'NSA' og 'GCHQ'). Hvilke typer organisationer er NSA og GCHQ? Hvilke folk ansætter de? Er det til at sige noget om, hvor meget forskning der foregår i disse organisationer?
b. Hvad er motivationen for henholdsvis forskere ved universiteterne og forskere i sikkerhedstjenesterne? Er der, og i så fald hvordan, forskel på 'sociologien' i disse to videnskabelige samfund?
c. Hvem synes I bør tildeles æren for henholdsvis offentlig-nøgle kryptering og RSA? Argumenter for jeres synspunkter.

Litteratur

Artmann, B. (1999). *Euclid – The Creation of Mathematics*, Springer-Verlag, New York.

Bass, T. A. (1995). Gene Genie, *Wired Magazine* **3**(08).

Bauer, F. L. (1997). *Decrypted Secrets – Methods and Maxims of Cryptology*, Springer, Berlin.

Biggs, N. L. (1989). *Discrete Mathematics*, Revised edn, Oxford Science Publications, Oxford.

Boyer, C. B. (1968). *A History of Mathematics*, John Wiley & Sons, New York.

Brousseau, G. (1997). *Theory of Didactical Situations in Mathematics*, Kluwer Academic Publishers, Dordrecht. Edited and translated by Nicolas Balacheff, Martin Cooper, Rosamund Sutherland, and Virgina Warfield.

Diffie, W. & Hellman, M. E. (1976). New Directions in Cryptography, *IEEE Transactions on Information Theory* pp. 29–40.

Euclid (1956). *Euclid's Elements*, second edn, Dover Publicatios, New York. Volume 2. Bog III-IX. Oversat og kommenteret af Sir Thomas L. Heath.

Gauss, C. F. (1986). *Disquisitiones Arithmeticae*, english edn, Springer-Verlag, New York. Udgivet på latin i 1801. Oversat til engelsk af Arthur A. Clarke og udgivet af Yale University Press i 1966.

Guy, R. K. (1994). *Unsolved Problems in Number Theory*, Problem Books in Mathematics – Unsolved Problems in Intuitive Mathematics, second edn, Springer-Verlag, New York.

Hansen, J. P. & Spalk, H. G. (2002). *Algebra og talteori*, Aspekt serien, Gyldendalske Boghandel, Nordisk forlag, København.

Hardy, G. H. & Wright, E. M. (1968). *An Introduction to the Theory of Numbers*, fourth edn, Oxford University Press, London.

Hardy, G. H. (1940). *A Mathematician's Apology*, Cambridge University Press.

Kahn, D. (1967). *The Codebreakers – The Story of Secret Writing*, The Macmillan Company, Toronto.

Katz, V. J. (1998). *A History of Mathematics – An Introduction*, second edn, Addision-Wesley Educational Publishers, Inc., Reading, Massachusetts.

Kjeldsen, T. H., Pedersen, S. A. & Sonne-Hansen, L. M. (2004). Introduction, *in* T. H. Kjeldsen, S. A. Pedersen & L. M. Sonne-Hansen (eds),

New Trends in the History and Philosophy of Mathematics, Vol. 19 of *Studies in Philosophy*, University Press of Southern Denmark, Odense, pp. 11–27.

Kline, M. (1972). *Mathematical Thoughts – From Ancient to Modern Times*, Oxford University Press, New York.

Levinson, N. (1970). Coding Theory: A Counterexample to G. H. Hardy's Conception of Applied Mathematics, *The American Mathematical Monthly* **77**(3): 249–258.

Menezes, A. J., van Oorschot, P. C. & Vanstone, S. A. (1997). *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida.

Nielsen, C. A., Saglanmak, N., Godiksen, R. B., Nielsen, S. M. H. & Eriksen, T. K. (1999). RSA – et sikkert kryptosystem? 4. semestersprojekt ved den Naturvidenskabelige Basisuddannelse, Roskilde Universitetscenter.

Niss, M. & Højgaard Jensen, T. (eds) (2002). *Kompetencer og matematiklæring – Ideer og inspiration til udvikling af matematikundervisning i Danmark*, Undervisningsministeriet. Uddannelsesstyrelsens temahæfteserie nr. 18.

Pomerance, C. (1982). The Search for Prime Numbers, *Scientific American* **247**(6): 136–144.

Rivest, R. L., Shamir, A. & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM* .

Rosen, K. H. (2003). *Discrete Mathematics and Its Applications*, fifth edn, McGraw Hill, New York.

Singh, S. (1999). *The Code Book – The Secret History of Codes and Codebraking*, Forth Estate, London.

Smith, D. E. (1925a). *History of Mathematics – Volume I*, Dover Publications, Inc., New York.

Smith, D. E. (1925b). *History of Mathematics – Volume II*, Dover Publications, Inc., New York.

Struik, D. J. (1969). *A Source Book in Mathematics, 1200-1800*, Harvard University Press, Cambridge, Massachusetts.

Undervisningsministeriet (2007). Vejledning: Matematik A, Matematik B, Matematik C. Bilag 35, 36, 37.
URL: *http://us.uvm.dk/gymnasie//vejl/*

van Tilborg, H. C. A. (2000). *Fundamentals of Cryptology – A Professional Reference and Interactive Tutorial*, Kluwer Academic Publishers, Massachusetts.

Weil, A. (1984). *Number Theory – An approach through history. From Hammurapi to Legendre*, Birkhäuser, Boston.

Wells, D. (2005). *Primtal Matematikkens gådefulde tal – fra A-Ø*, Nyt Teknisk Forlag, København. Oversat til dansk af Poul G. Hjorth.

Yong, L. L. & Se, A. T. (1992). *Tracing the Conceptions of Arithmetic and Algebra in Ancient China – Fleeting Footsteps*, second edn, World Scientific Publishing, Singapore.